*فصلنامه علمی امنیت ملی*
*سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹*
*مقاله یازدهم از صفحات ۳۸۶-۳۵۳*

# مقاله پژوهشی: ارائه مدل فرایندی دفاع سایبری بومی

حسین امیرلی[۱]، رضا تقی‌پور[۲]

**تاریخ دریافت:۱۳۹۷/۰۵/۱۰** **تاریخ پذیرش:۱۳۹۸/۰۵/۲۶**

## چکیده

گسترش روزافزون فضای سایبر سبب شده است که بخش قابل توجهی از فعالیت‌های حاکمیتی ازجمله فعالیت‌های امنیتی و نظامی به این فضا منتقل و فضای مزبور به عرصه نبرد مبدل شود؛ بنابراین به‌منظور صیانت از منافع کشور ضرورت دارد ساختار یکپارچه و بومی برای دفاع در این فضا فراهم گردد. فرایندهای اصلی یا کلیدی از مهم‌ترین مباحث دفاع سایبری محسوب می‌شوند که دفاع پیرامون آن‌ها شکل می‌گیرد. برای دستیابی به فرایندهای اصلی دفاع سایبری در این پژوهش، با بهره‌گیری از روش موردی زمینه‌ای، نخست اسناد بالادستی کشور مورد مطالعه قرار گرفته و با گزینش چند کشور، اسناد راهبردی قابل دسترس این کشورها بررسی شد و با ورود گزاره‌های استخراج‌شده از آن‌ها در سطح راهبردی، چارچوب معماری زکمن و با بهره‌گیری از دانش ۱۴ نفر از خبرگان این حوزه از طریق مصاحبه و پرسشنامه، فرایندهای کلیدی دفاع سایبری احصاء و با استفاده از روش مدل ساختاری تفسیری و مقایسه‌ای زوجی، این فرایندها سطح‌بندی و ارتباط بین آن‌ها ترسیم و مدل نهایی ارائه گردیده است.

**کلیدواژه‌ها:** دفاع سایبری، فرایند، معماری، مدل ساختاری تفسیری و مقایسه زوجی

۱. دانش‌آموخته دوره دکتری مدیریت راهبردی فضای سایبر (نویسنده مسئول) ایمیل: h.amirli@chmail.ir
۲. دانشیار دانشگاه عالی دفاع ملی taghipour@sndu.ac.ir

**مقدمه**

با توسعه روزافزون فضای سایبر، بیش‌ازپیش فعالیت‌های روزمره بشر به این فضا وابستگی پیدا می‌کند؛ زیرساخت‌های مهم، حساس و حیاتی نیز از این قاعده مستثنا نمی‌باشند و بیش از گذشته به فضای سایبر وابسته شده‌اند. سامانه‌های اطلاعاتی و مخابراتی، نیروگاه‌ها (برق‌آبی، هسته‌ای، گازی)، پالایشگاه‌ها و خطوط انتقال حامل‌های انرژی، سامانه‌های بانکی و مالی، سامانه‌های حمل‌ونقل (هوایی، جاده‌ای، ریلی و دریایی)، خدمات بهداشتی و اضطراری، صنایع دفاعی و شبکه آب‌رسانی، هشت زیرساخت عمده می‌باشند که در سطح جهان شناسایی شده‌اند (Stevens, 2003). در کشور ما نیز این زیرساخت‌ها و سامانه‌ها یا خود، بخشی از فضای سایبری هستند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور، به این فضا منتقل می‌شود و یا اساساً در این فضا، شکل گرفته است؛ این فضا به‌عنوان زیرساخت سایر زیرساخت‌های کشور قلمداد شده و قسمتی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه می‌شود.

بررسی سوابق جنگ‌ها و انقلاب‌های مخملی شکل‌گرفته طی دو دهه اخیر، در سطح جهان که منجر به براندازی حکومت‌ها و نابودی منابع و زیرساخت‌های آن‌ها شده است، بیانگر این واقعیت است که تعدادی از این جنگ‌ها و انقلاب‌ها، با یک جنگ و اقدام سایبری شروع و یا حمایت شده است. مروری بر وقایع و حوادث سال‌های اخیر کشور، مؤید این واقعیت است که بخش اعظم تهدیدهای موجود علیه کشور، به‌ویژه در زیرساخت‌های حیاتی یا از فضای سایبر نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند. در جنگ‌های قبلی عناصر زیرساختی حیاتی از قبیل فرودگاه، نیروگاه‌های برق، سامانه‌های آب، راه‌آهن، خطوط لوله نفت و گاز و مراکز ارتباطی به‌وسیله نیروهای نظامی مورد هدف قرار می‌گرفتند؛ زیرا انهدام آن‌ها می‌توانست به فلج شدن یک کشور کمک کند. این مراکز کنترل، همان اجزایی هستند که دیگر به‌صورت فیزیکی وجود ندارند و بیشتر آن‌ها به سامانه‌های رایانه‌محور وابسته شده‌اند که به‌سادگی

می‌توانـد از طریـق یـک حملـه سـایبری غیرفعـال گـردد(Kamal, 2005:76). در محافـل بین‌المللی اغلب صحبت از امکان حملات سایبری در میان است. اسـتفاده از سـلاح‌هـای سایبری می‌تواند بـه‌عنـوان وسـیله‌ای ارزان بـرای برخـی از کشـورها و همچنـین بـرای گروه‌های مجرمانه و تروریستی، جذابیت داشته باشـد. تهدیـد حمـلات سـایبری آن‌قـدر جدی است که پیمان آتلانتیک شمالی (ناتو) در نسخه جدید راهبردهای خود بـه مسـئله «تبدیل فضای مجازی به میدان جنگ» پرداخته است، چراکه با افزایش وابستگی کشـورها به فضای سایبر، زمینه آسیب‌پذیری ناخواسته در برابر حملات و تهدیدهای سـایبری نیـز شدت می‌یابد.

محور قرار گرفتن فضای اطلاعاتی و سـایبری در سـاختارها، اگرچـه باعـث افـزایش چشمگیر کارایی، انعطاف‌پذیری، نوآوری و تحول می‌شود، لیکن از طرف دیگر می‌توانـد به نقطه‌ضعف عمـده کشـور مبـدل گـردد. پـژوهش حاضـر گـامی در راسـتای پوشـش نقطه‌ضعف یادشده به شمار می‌رود؛ بنابراین در باب اهمیت تحقیق می‌توان گفـت: الـف. انجام آن سبب کمک علمی به حوزه تصمیم‌سازی و تصمیم‌گیـری دفـاع سـایبری کشـور می‌شود. ب. بستر لازم را برای تفکر در مدل دفاع سایبری بومی کشور فراهم مـی‌نمایـد. ج. خلأ دانشی را در کشور پیرامون دفاع سایبری پوشش می‌دهد و موجب فرهنگ‌سـازی در حوزه دفاع سایبری بومی برای الگوبرداری نهادهای مرتبط می‌گردد.

در باب ضرورت تحقیق می‌توان گفت: هر پژوهشی بستر تحقیقات پیوسته مـرتبط را فراهم می‌نماید، بنابراین بدون انجام پـژوهش حاضـر، زمینـه موصـوف بـرای تحقیقـات مشابه در حوزه دفاع سایبری شکل نمی‌گیرد و همچنین تا سالیان متمـادی ممکـن اسـت وظایف نهادهای کشور در دفاع سایبری تبیین نگردد و به‌طورکلی ممکن اسـت هـرگونـه غفلت از این تحقیق یا پژوهش‌های مشابه در مقوله دفـاع سـایبری، لطمـات و خسـارات جبران‌ناپذیری را بر پیکره زیرساخت‌های موصوف به‌عنوان مراکز ثقل کشور وارد نمایـد، مضاف بر آنکه خاستگاه عمده فناوری‌های این فضا، کشورها و قدرت‌هـایی هسـتند کـه بی‌واسطه یا باواسطه دارای تضاد منـافع در حـوزه سیاسـی، اقتصـادی، دینـی و غیـره بـا

کشورمان می‌باشند؛ بنابراین ضرورت شکل‌دهی و ایجاد یک نظام دفـاعی بـومی، بـه‌روز، همیشه بیدار، قدرتمند و آینده‌نگر برای تضمین و استمرار فعالیت کشور در فضای سایبر به‌ویژه فعالیت‌های حاکمیتی بیش‌ازپیش نمایان می‌شـود. ایـن پـژوهش بـا هـدف اصـلی «تدوین مدل فرایندی دفاع سایبری بومی کشور» و اهداف فرعی «شناخت اسناد بالادستی موجود در این زمینه» و «شناخت ارکان جهت‌ساز و راهبردهای دفاع سایبری کشـورهای مورد مطالعه» به‌منظور پاسخ‌گویی به این سؤال که «فرایندهای اصلی دفاع سـایبری بـومی کشور کدامند؟» و سؤالات فرعی «اسـناد بالادسـتی در ایـن زمینـه کدامنـد؟» و همچنـین «ارکان جهت‌ساز و راهبردهای دفاع سایبری کشـورهای مـورد مطالعـه چگونـه اسـت؟» تنظیم گردیده و بر آن است که گامی هرچند کوچک در این مسیر بردارد.

## مبانی نظری

در این بخش نخست کلیدواژه اصلی مبحـث تبیـین مـی‌گـردد و در ادامـه بـه اسـناد بالادستی در زمینه دفاع، دفاع سایبری و همچنـین مطالعـات تطبیقـی در اسـناد راهبـردی سایر کشورها برای دستیابی به فرایندهای اصلی دفاع سایبری با استفاده از چارچوب‌های معماری پرداخته خواهد شد.

### دفاع

دفاع، در لغت‌نامه معین، از دستبرد دشمن حفظ کـردن، بازداشـتن، پـس زدن، پاسـخ طـرف مقابل در هر دعوی و جنگی که مسلمانان با کافران کنند بـرای جلـوگیری از حملـه آنـان (معـین، ۱۳۸۲: ۵۳۰) و در لغت‌نامه دهخدا، دور کردن از کسی، دفـع کـردن از کسـی، همـدیگر را رانـدن، مزاحم کسی شدن، دارا دار کردن حق کسـی را، یـاوری و حمایـت کـردن کسـی را از دسـتبرد دشمن (انسان و حیوان) حفظ کردن، بازداشتن و پس زدن(دهخـدا،۱۰۹۴۰: ۱۳۷۷) معنی شـده اسـت. دفاع در اصطلاح به مجموعه اقدامات بازدارنده، رفع‌کننده، دفع‌کننده و بازیابی‌کننده که بـه‌منظـور پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملـی در مقابـل تهدیـدات و حمـلات انجام می‌گیرد گفته می‌شود (رامک و همکاران، ۱۳۹۵).

### دفاع سایبری

به‌کارگیری اقدامات حفاظتی مؤثر برای به دست آوردن یک سطح مناسب از امنیت سایبری به‌منظور تضمین عملکرد و عملیات دفاعی. این موضوع به‌وسیله اقدامات محافظتی مناسب برای کاهش مخاطره امنیتی به یک سطح قابل پذیرش حاصل می‌شود. دفاع سایبری از وظایف و تکالیف، حفاظت،[1] کشف،[2] پاسخ[3] و بازیابی[4] تشکیل شده است (ACST–Strategy-CyberSecurity, 2014: 18). این تعریف به‌عنوان تعریف عملیاتی ارائه شده است.

### زیرساخت‌های حیاتی

تعریف عملیاتی: سازمان‌ها و یا تأسیسات باارزش و اساسی می‌باشند که شکست یا تخریب آن‌ها منجر به تنگناهای تأمین پایدار، اخلال قابل توجه در امنیت عمومی یا سایر نتایج تلخ دیگر خواهد شد. مواردی چون انرژی، فناوری اطلاعات و ارتباطات، انتقال، سلامتی، آب، غذا، بخش امور بیمه و مالی، دولت و بخش اجرایی، رسانه و فرهنگ به‌عنوان زیرساخت‌های حیاتی، شناسایی شده‌اند (مؤسسه آموزشی و تحقیقاتی صنایع، ۱۳۹۰: ۵۶).

### فرایند

فرایند عبارت است از مجموعه‌ای از مراحل، فعالیت‌ها و وظایف هدفمند که با استفاده از زیرساخت‌های لازم و روش‌های خاص، یک یا چند ورودی را به یک یا چند خروجی تبدیل می‌کند (ISO 9001, 2000). این تعریف نیز به‌عنوان تعریف عملیاتی پذیرفته شده است.

1. Protect
2. Detect
3. Respond
4. Recover

**معماری سازمانی**

تعریف عملیاتی: هرجا که نیاز به طراحی موجودیت یا سامانه‌ای باشد که ابعاد و پیچیدگی آن از حد معینی فراتر رفته یا نیازمندی‌های خاصی را تحمیل نماید، نگرش ویژه و همه‌جانبه‌ای را نیاز خواهد داشت که در اصطلاح به آن «معماری» گفته می‌شود. معماری ترکیبی از علم، هنر و تجربه است که در رشته‌هایی نظیر ساختمان دارای قدمتی چند هزارساله است (شمس، ۱۳۸۳).

تدوین فرایندهای مطلوب برای دفاع سایبری با مطالعه ارزش‌های اساسی جامعه و اسناد بالادستی کشور و از طرف دیگر با مطالعات تطبیقی و بهره‌گیری از تجربیات سایر کشورها امکان‌پذیر خواهد بود که در ادامه مقاله به این مهم می‌پردازیم.

مطالعه اسناد بالادستی

اسنادی که برای تدوین فرایندهای دفاع سایبری مورد مطالعه قرار گرفته و کلیدواژه‌های آن‌ها استخراج گردید عبارت‌اند از: آیات قرآن مجید، فرمایشات امام خمینی(ره)، فرمایشات حضرت امام خامنه‌ای(مدظله‌العالی)، سند سیاست‌های کلی نظام در چشم‌انداز جمهوری اسلامی ایران، سند امنیت فضای تولید و تبادل اطلاعات (افتا)، سند راهبردی پدافند سایبری کشور، قوانین داخلی در خصوص دفاع، برخی از شرح وظایف و اختیارات شورای عالی فضای مجازی، اهداف و سیاست‌های شورای عالی فضای مجازی. در این بخش نخست از دیدگاه دین مبین اسلام و منظر حضرت امام خمینی(ره) و حضرت امام خامنه‌ای(مدظله‌العالی) به موضوع دفاع وارد می‌شویم:

**دفاع درآیات و احادیث**

بررسی آیات قرآن و روایات اسلامی در مورد آداب دفاع این حقیقت را به‌وضوح ثابت می‌کند که اسلام مسائل اخلاقی و انسانی را حتی در خشونت‌بارترین صحنه‌های زندگی؛ یعنی میدان جنگ و دفاع نادیده نگرفته و همه‌جا قهر را با لطف و خشونت را با

رحمت، عجین ساخته و به‌یقین حکومت اسلامی باید این آداب را که اثر عمیقی در طرز قضاوت بیگانگان از اسلام دارد و می‌تواند وسیله‌ای برای جلب توجه آنان و بازنگری درباره اسلام شود به کار بندد. در آیات قرآن بارها به رعایت عدالت و عدم تجاوز از حدود معقول و انسانی در مقابل دشمنان تأکید شده است. ازجمله در آیات ۱۹۰ تا ۱۹۵ سوره بقره می‌خوانیم: «و در راه خدا با کسانی که با شما سر جنگ دارند کارزار بکنید اما تعدی روا مدارید که خدا متجاوزان را دوست نمی‌دارد. (۱۹۰) و ایشان را هر جا که دست یافتید به قتل برسانید و از دیارشان مکه بیرون کنید، همان‌طور که شما را از مکه بیرون کردند و فتنه آنان از این کشتار شما شدیدتر بود ولی در خود شهر مکه که خانه امن است با ایشان نجنگید مگر اینکه ایشان در آنجا با شما جنگ بیاغازند که اگر خود آنان حرمت مسجدالحرام را رعایت ننموده و جنگ را با شما آغاز کردند، شما هم بجنگید که سزای کافران همین است. (۱۹۱) حال اگر از شرارت و جنگ در مکه دست برداشتند، شما هم دست بردارید که خدا آمرزگاری رحیم است. (۱۹۲) و با ایشان کارزار کنید تا به‌کلی فتنه ریشه‌کن شود و دین تنها برای خدا شود و اگر به‌کلی دست از جنگ برداشتند دیگر هیچ دشمنی و خصومتی نیست مگر علیه ستمکاران. (۱۹۳) اگر آنان حرمت ماه حرام را شکستند شما هم بشکنید چون خدا قصاص را در همه حرمت‌ها جایز دانسته پس هرکس بر شما ستم کرد، شما هم به همان اندازه که بر شما ستم روا داشتند بر آنان ستم کنید و نسبت به ستم بیش از آن از خدا بترسید و بدانید که خدا با مردم باتقوا است. (۱۹۴) و در راه خدا انفاق کنید و خویشتن را به دست خود به هلاکت نیفکنید و احسان کنید که خدا نیکوکاران را دوست دارد». (۱۹۵) سیاق آیات شریفه دلالت دارد بر اینکه همه یک‌باره و باهم نازل شده و اینکه همه یک غرض را ایفا می‌کنند و آن عبارت است از: فرمان جنگ برای اولین بار با مشرکین مکه و اینکه می‌گوییم با خصوص مشرکین مکه، از اینجا می‌گوییم که در این آیات به ایشان تعرض شده که مؤمنین را از مکه بیرون کردند و نیز متعرض مسئله فتنه و امر قصاص است و نیز نهی می‌فرماید از اینکه این جنگ را پیرامون مسجدالحرام انجام دهند، مگر اینکه مشرکین در

آنجا جنگ را آغاز کنند و همه این‌ها اموری است مربوط به مشرکین مکه. علاوه بر این در این آیات، قتال را مقید به قتال کرده و فرموده «و قاتلوا فی سبیل اللّه، الذین یقاتلونکم؛ در راه خدا قتال کنید با کسانی که با شما قتال می‌کنند». معلوم است که معنای این کلام اشتراط قتال به قتال نیست و نمی‌خواهد بفرماید اگر قتال کردند شما هم قتال کنید، چون در آیه کلمه «ان- اگر» به کار نرفته، از سوی دیگر قید نامبرده احترازی هم نمی‌تواند باشد تا معنا این شود که تنها با مردان قتال کنید نه با زنان و کودکان لشکر دشمن، (که بعضی این‌طور معنا کرده‌اند) برای اینکه قتال با زنان و اطفال که قدرت بر قتال ندارند عملی بی‌معنا است و معنا ندارد بفرماید با آنان مقاتله (جنگ طرفینی) مکن، بلکه اگر منظور این بود باید بفرماید: «زنان و کودکان را مکشید».

بنابراین می‌توان نتیجه گرفت که قرآن مجید در جنگ و دفاع نیز عدول از حدود معقول انسانی را جایز ندانسته و با تحدید مکرر آن به مکان و زمان حرام و همچنین مقاتله با زنان و کودکان و همچنین آغاز جنگ، با وسواس خاصی ابعاد آن را مشخص نموده است که ضرورت دارد در فرایندهای دفاع سایبری نیز لحاظ گردد.

### دفاع از دیدگاه امام خمینی(ره)

به همان میزان که دفاع مقدس از فرهنگی جامع برخوردار است و پیام‌های گوناگون به نسل امروز منتقل می‌سازد و پشتوانه‌های نیرومند فکری، اعتقادی، فرهنگی، اخلاقی و نظامی به وجود می‌آورد، تفکرات و رهنمودهای حضرت امام خمینی(ره) درباره دفاع مقدس نیز دارای جامعیت موضوع و درس‌ها و پیام‌های ماندگار و تحول‌زا است. افکار و رهنمودهای ژرف امام خمینی(ره) را نه‌تنها نمی‌توان مجزا و منفک از فرهنگ دفاع مقدس دانست که از عوامل مهم و ایجادکننده این فرهنگ غنی به شمار می‌رود و این عامل به‌گونه‌ای محوری و بنیادی است که اگر آن را از دفاع مقدس جدا کنیم، آنچه باقی می‌ماند فاقد ارزشمندی است و به‌هیچ‌وجه نمی‌تواند به این فرهنگ، جامعیت ببخشد و ذخیره‌سازی ارزش‌ها و اتقان و استحکام پشتوانه‌های فکری و عملی آن را محقق گرداند.

دفاع در اندیشه امام خمینی(ره) ماهیتی الهی و انسانی دارد. بدین‌جهت است که به تعبیر ایشان حضور توده مردم در صحنه جهاد و دفاع در جهت اطاعت خدا مطرح است. در راستای چنین برداشتی از ماهیت دفاع است که پیروزی‌های به‌دست‌آمده در میدان نبرد با دشمن در هشت سال دفاع مقدس را از جانب خدای سبحان دانسته و می‌گوید: بارالهی، جوانان رزمنده ایران فتح را از تو می‌دانند و به قدرت خویش مغرور نیستند و اگر غرور و سرفرازی هست، تو نازل فرمودی و رعب و وحشت را در قلوب دشمنان آنان که دشمنان اسلام‌اند، انداختی (صحیفه امام، ۱۳۸۹، ج ۱۶: ۸۶). ایده و تفکر امام خمینی(ره) برگرفته از مکتب دفاعی الهی اسلام است که ساختار و دکترین آن را عاشورایی اندیشیدن شکل می‌دهد. ازاین‌رو، معیار پیروزی و شکست، انجام تکلیف است؛ بدین معنی که اگر به تکلیف عمل شود، پیروزی به دست آمده است و اگر به تکلیف عمل نشود، ولو در ظاهر پیروزی به دست آمده باشد، اما درواقع شکست است؛ بنابراین معیار پیروزی، ادای تکلیف است. بدین‌جهت است که امام خمینی(ره) معتقد است ما در جنگ برای یک لحظه هم نادم و پشیمان از عملکرد خود نیستیم. راستی مگر فراموش کرده‌ایم که برای ادای تکلیف جنگیده‌ایم و نتیجه فرع آن بوده است(صحیفه امام، ج ۲۱: ۱۰۲–۸۸). در راستای چنین بینشی نسبت به هدف از دفاع و جهاد در راه خداست که می‌فرماید: جنگ ما جنگ ایمان و رذالت بود و این جنگ از آدم تا ختم زندگی وجود دارد(صحیفه امام، ج ۲۱: ۲۸۴).

امام خمینی(ره) در اولین بیان صریح در باب دفاع همه‌جانبه، بلافاصله بعد از اشاره به این راهبرد، سخن از بسیج می‌گوید و معتقد است اگر بر کشوری ندای دل‌نشین تفکر بسیجی طنین اندازد، چشم طمع دشمنان و جهانخواران از آن دور خواهد گردید والا هر لحظه باید منتظر حادثه باشیم. (صحیفه امام، ۱۳۸۹، ج ۲۱: ۵۲)

از نظر امام کارویژه دفاعی بسیج، به‌ویژه در عرصه بازدارندگی، منحصر به سیاست‌های امنیتی جمهوری اسلامی نبوده و گستره‌ای فراملی و جهانی را در برمی‌گیرد. من امیدوارم که این بسیج عمومی اسلامی، الگو برای تمام مستضعفین جهان و ملت‌های مسلمان عالم باشد و قرن پانزدهم، قرن شکستن بت‌های بزرگ و جایگزینی اسلام و

توحید به‌جای شرک و عدل به‌جای ستمگری و بیدادگری و قرن انسان‌های متعهد به‌جای آدم‌خواران بی‌فرهنگ باشد(صحیفه امام، ۱۳۸۹، ج ۲۱: ۵۲).

مهم‌ترین مفاهیم بنیادی در بیانات ایشان عبارت از فرهنگ عاشورایی در دفاع، نقش بسیج، دفاع همه‌جانبه، عرصه دفاع و ماهیت انسانی و الهی دفع می‌باشد. در ادامه به دفاع از منظر حضرت امام خامنه‌ای(مدظله‌العالی) که برگرفته از اندیشه‌های بلند امام راحل(ره) و آیات قرآن مجید و روایات ائمه معصوم است می‌پردازیم.

## دفاع از دیدگاه حضرت امام خامنه‌ای(مدظله‌العالی)

از نگاه امام خامنه‌ای، دفاع و امنیت ملی همان فرایند گسترده حفظ دستاوردهای انقلاب اسلامی و دستیابی به آرمان‌های متعالی و هموار ساختن مسیر رشد و تعالی مرهون توسعه اقتدار روزافزون سیاسی، فرهنگی، اقتصادی، اجتماعی و نظامی است تا بتواند با بهره‌گیری از تمام ظرفیت‌ها، امکانات و استعدادهای درونی، بحران‌های ناخواسته داخلی و تهدیدهای دشمنان خارجی را یکی پس از دیگری خنثی کند و به سلامت به سرمنزل مقصود برسد؛ بنابراین به‌صراحت می‌توان گفت که پرداختن همه‌جانبه به مقوله ابعاد مؤلفه‌های امنیت ملی و دوری از چالش‌ها و دفع تهدیدها در شرایط کنونی و حساس نظام، مهم‌ترین موضوعی است که شایسته است در دستور کار کارگزاران نظام اسلامی قرار گیرد. ایشان، مسیر صعود به قله افتخارات کشور را عبور از پله‌های امنیت ملی می‌دانند. بیانات گوناگون معظم‌له(www.khamenei.ir) که در این رابطه مورد بررسی قرار گرفته در جدول زیر نشان داده شده است:

**جدول (۱) فرمایشات حضرت امام خامنه‌ای(مدظله‌العالی) در مناسبت‌های گوناگون پیرامون دفاع**

| ردیف | مکان |
|---|---|
| ۱ | در دیدار با جمعی از کارکنان نیروی هوایی ارتش جمهوری اسلامی به مناسبت روز نیروی هوایی ۱۳۶۹/۱۱/۱۹ |
| ۲ | در مراسم ششمین دوره فرماندهی و ستاد دانشگاه امام حسین (علیه‌السلام)۱۳۶۸/۸/۲۹ |
| ۳ | در مراسم مشترک نیروهای مسلح استان کردستان ۱۳۸۸/۲/۲ |
| ۴ | در دیدار با فرماندهان گردان های عاشورای نیروهای مقاومت بسیج در سالروز شهادت امام سجاد(ع) ۱۳۹۳/۵/۱۲ |
| ۵ | در دیدار با مردم مازندران در سالگرد حماسه ۶ بهمن ۱۳۸۸/۱۱/۶ |
| ۶ | در مراسم بیعت با فرماندهان و مسئولان سپاه پاسداران انقلاب اسلامی۱۳۶۸/۴/۱۹ |
| ۷ | در مراسم صبحگاه نظامی پایگاه منطقه دوم دریایی نیروی دریایی ارتش در بوشهر ۱۳۷۰/۱۰/۱۲ |
| ۸ | در جمع دانشجویان و فارغ‌التحصیلان دانشگاه علوم نظامی ۱۳۶۹/۷/۱۴ |
| ۹ | در مراسم سالگرد ارتحال حضرت امام(ره) ۱۳۷۱/۰۳/۱۴ |
| ۱۰ | در مراسم اعطای سردوشی به فارغ‌التحصیلان دوره‌های فرماندهی و علوم نظامی ارتش ۱۳۶۸/۷/۱۳ |
| ۱۱ | در دیدار گروهی از معلمان و فرهنگیان و جمعی از کارگران در تقارن روز معلم و روز جهانی کارگر ۱۳۶۹/۲/۱۲ |
| ۱۲ | در بازدید سرزده از دانشگاه افسری امام علی (علیه‌السلام) – ۱۳۸۳/۰۱/۳۰ |
| ۱۳ | ابلاغ سیاست‌های کلی برنامه پنجم توسعه در چارچوب سند چشم‌انداز بیست‌ساله ۱۳۸۷/۱۹/۲۱ |

سخنرانی‌ها و فرمایشات حضرت امام خامنه‌ای(مدظله‌العالی) در خصوص مقوله دفاع (سخنرانی‌های اشاره‌شده در جدول شماره ۱) توسط محققین مورد بررسی دقیق و تحلیل محتوا قرار گرفته و کلیدواژه‌های مؤثر در حوزه دفاع از آن‌ها استخراج و در جدول شماره (۲) درج گردید:

**جدول (۲): موارد مستخرج از فرمایشات امام خامنه‌ای(مدظله‌العالی) در خصوص مقوله دفاع**

| | مفاهیم قابل استخراج از فرمایشات ایشان در خصوص دفاع | مؤلفه‌های مؤثر در نظام دفاع سایبری برگرفته از بیانات ایشان |
|---|---|---|
| مواردی که می‌بایست از آن‌ها دفاع کرد | - اسلام و قرآن و انقلاب<br>- نظام جمهوری اسلامی<br>- عقاید و ارزش‌ها و موجودیت<br>- حیثیت و عزت کشور<br>- حاکمیت تمامیت ارضی<br>- منافع و امنیت ملی<br>- حقوق مردم، حقوق سیاسی و اقتصادی<br>- جایگاه شایسته بین‌المللی<br>- مستضعفین و مظلومین<br>- اسلام بیدارشده<br>- ملت‌های به هویت اسلامی برگشته<br>- ملت‌های فلسطین و لبنان<br>- حوزه‌های اخلاقی، دینی و نظامی | - نظام دفاع سایبری می‌بایست در راستای صیانت از حقوق و ارزش‌های اساسی و اسلامی باشد. |
| ویژگی‌های دفاع | - دانش و کسب فناوری<br>- شناسایی و ارزیابی دشمن<br>- برگزاری مانور<br>- سازمان‌دهی و کار و تلاش<br>- روحیه و آمادگی<br>- خودباوری و اتکا به خود<br>- نوآوری، آموزش، انضباط<br>- وحدت و یکپارچگی | - نظام دفاع سایبری می‌بایست مبتنی بر دانش و فناوری روز باشد.<br>- نظام دفاع سایبر می‌بایست متناسب با توان دشمنان طراحی گردد.<br>- ارزیابی مستمر و حفظ آمادگی بخش‌های مختلف می‌بایست بخشی از فرایندهای نظام دفاع سایبری باشد.<br>- وحدت فرماندهی و مدیریت یکپارچه از ویژگی‌های نظام دفاع سایبری است.<br>- نظام دفاع سایبری نیازمند آموزش مستمر در کلیه لایه‌های مؤثر است.<br>- تثبیت نظام دفاع سایبری با توجه به تغییرات مداوم فضای سایبر نیازمند ارتقاء خلاقیت و نوآوری است.<br>- خودباوری و خوداتکایی در فناوری و فرایندهای نظام دفاع سایبری دارای اهمیت ویژه‌ای است. |

| | مفاهیم قابل استخراج از فرمایشات ایشان در خصوص دفاع | مؤلفه‌های مؤثر در نظام دفاع سایبری برگرفته از بیانات ایشان |
|---|---|---|
| عوامل مؤثر در دفاع | - استفاده از کلیه ظرفیت‌های کشور<br>- ارتقاء قدرت بازدارندگی و قدرت دفاعی<br>- توجه به جوانان<br>- خودباوری و اتکا به خود<br>- باور دفاع دائمی<br>- آمادگی دفاعی برای همگان<br>- آمادگی دفاعی هر زمان و هر مکان<br>- جایگزینی رویکرد فعال به‌جای منفعل | - بهره‌گیری از کلیه ظرفیت‌های کشور در نظام دفاع سایبری<br>- ایجاد قدرت بازدارندگی در ساختار نظام دفاع سایبری<br>- نظام دفاع سایبری با نقش‌آفرینی آحاد ملت<br>- نظام دفاع سایبری رویکردی فعال دارد<br>- نظام دفاع سایبری هر زمان هر کجا |
| ملاحظات دفاعی | - توجه به وضعیت دفاعی در ساخت ابنیه و امکانات زیربنایی و زیرساختی و حیاتی<br>- ارتقاء قدرت<br>- گاهی دفاع با فهمیدن است (دانش)<br>- گاهی دفاع با زبان است (بیان و اطلاع‌رسانی)<br>- گاهی دفاع با حضور در جایی است (آمادگی)<br>- قدرت دفاعی باید متناسب با داعیه‌ها و آرمان‌های انقلاب باشد<br>- قدرت دفاعی نقش مؤثری در تعیین جایگاه و معادلات جهانی دارد<br>- آنچه در تاریخ مایه افتخار ملت‌هاست، قدرت دفاع و قدرت سازندگی اوست<br>- تهدید همیشگی است، حتی اگر منجر به جنگ نشود<br>- حفظ سرمایه‌های مادی و معنوی متضمن دفاع<br>- دفاع به معنای تجاوز نیست<br>- آمادگی دفاعی به مفهوم زنده بودن یک ملت است<br>- دفاع جزئی از هویت یک ملت است<br>- توجه به اهمیت و گسترش پدافند غیرعامل | - در ساخت و ایجاد زیرساخت‌های سایبری کشور ملاحظات نظام دفاع سایبری باید رعایت گردد.<br>- آموزش و گسترش آگاهی از ارکان نظام دفاع سایبری است.<br>- نظام دفاع سایبری می‌بایست با توجه به هدف قرار داشتن کشور در سیاست‌های استعماری طراحی گردد.<br>- در نظام دفاع سایبری آفند قرار ندارد.<br>- نظام دفاع سایبری متضمن صیانت از سرمایه‌های مادی و معنوی کشور است. |

سایر اسناد بالادستی نیز مانند سند سیاست‌های کلی نظام در چشم‌انداز جمهوری اسلامی ایران، سند امنیت فضای تولید و تبادل اطلاعات (افتا)، سند راهبردی پدافند سایبری کشور، قوانین داخلی در خصوص دفاع، برخی از شرح وظایف و اختیارات شورای عالی فضای مجازی، اهداف و سیاست‌های شورای عالی فضای مجازی با روش مشابه مورد بررسی قرار گرفته و کلیدواژه‌های آن‌ها استخراج و گزاره مورد نیاز در حوزه دفاع سایبری تبیین و در جداولی جمع‌بندی شده و مانند سایر اسناد در سلول‌های چارچوب زکمن برای تدوین فرایندهای دفاع سایبری مورد بهره‌برداری قرار گرفتند.

**مطالعات تطبیقی در سایر کشورها**

شیوه و روش مطالعات تطبیقی امروزه در گستره علوم انسانی از اهمیت بسیار بالایی برخوردار است. به‌طوری‌که بسیاری از محققان بر این امر واقف‌اند که این شیوه مطالعاتی نکات مهمی از گستره را مورد نقد و بازخوانی قرار می‌دهد. از نظر نباید دور داشت که تحولات فکری همان‌گونه که مرهون تأثیرپذیری درونی است می‌توانند متأثر از مراودات و برگرفته از بیرون نیز باشند. مقایسه مسئله امنیت و دفاع در فضای سایبر با مسائل متعدد آن در چند کشور و تبیین مواضع مشترک و مختلف، می‌تواند نگرش شناختی را نیرومندتر و جامع‌تر سازد. بر اساس معیارهایی چون بازیگران اصلی فضای سایبر (پدیدآورندگان)، کشورهای پیشرو، کشورهای منطقه، اتحادیه‌ها و سازمان‌های بین‌المللی مصادیقی را برای این مطالعه تطبیقی ارائه می‌نمایند که از میان آن‌ها آمریکا، انگلیس، استرالیا، اتحادیه اروپا، رژیم صهیونیستی، کره جنوبی و ترکیه با شاخص‌های دکترین، چشم‌انداز، ارزش‌ها، اهداف، سیاست‌ها، مأموریت، ساختار، راهبرد و اقدامات در مطالعات مورد بررسی قرار گرفت. البته گفتنی است که پرداختن به اسناد راهبردی و ارکان جهت‌ساز در آن‌ها به علت عدم انتشار فرایندهای دفاع سایبری در کشورهای یادشده صورت گرفته و تلاش گردیده با استخراج کلیدواژه‌های مهم اسناد راهبردی آن‌ها، بخش‌هایی از دفاع سایبری که بیشترین توجه به آن‌ها معطوف شده است مورد

توجه قرار گیرد. البته این نکته را نیز از نظر نباید دور داشت که رویکرد اغلب این کشورها به حوزه‌های امنیت و دفاع با رویکرد جمهوری اسلامی ایران متمایز بوده و دارای تفاوت‌های اساسی است.

در راستای سازمان‌دهی مطالعه تطبیقی، پس از تشکیل لیست کشورهای قابل مطالعه (متشکل از ۳۳ کشور)، قدم بعدی جهت رسیدن به هفت‌کشور ارجح، پالایش کشورهای موصوف بر اساس سیاست‌های ذکرشده و اسناد راهبردی امنیت و دفاع سایبر قابل دسترس آن‌ها صورت گرفت و در ادامه از میان فهرست کشورهای قابل مطالعه و منطبق با سیاست‌های ترسیم‌شده، مطالعات تطبیقی که در سطور قبل بیان گردید، فهرست کشورهای ارجح برابر بندهای زیر به دست آمد:

- آمریکا (پیشروترین کشور در امنیت و دفاع سایبر که دارای اسناد راهبردی امنیت و دفاع سایبری است).
- انگلیس، استرالیا (کشور پیشرو در امنیت و دفاع سایبر و دارای اسناد راهبردی امنیت و دفاع سایبری).
- کره جنوبی (به‌عنوان کشوری در آسیا که در زمینه دفاع سایبری فعالیت‌های خوبی داشته است).
- ترکیه (کشوری در همسایگی جمهوری اسلامی ایران و مطابقت نسبی با ویژگی‌های فرهنگی کشور ایران که باید فعالیت‌های دفاع سایبری آن را رصد کرد).
- رژیم صهیونیستی (اهمیت این رژیم به دلیل دشمنی با جمهوری اسلامی و فعال در زمینه‌های دفاع سایبری مشخص است).
- اتحادیه اروپا (این اتحادیه برای حفظ یکپارچگی کشورهای اروپایی به موضوع دفاع سایبری کشورهای عضو، اهمیت ویژه‌ای داده است).

روشی که جهت انجام مطالعات تطبیقی مورد استفاده قرار گرفته در جدول (۳) نشان داده شده است.

**جدول (۳) جمع‌بندی یافته‌های مطالعات تطبیقی**

| کشور | چشم‌انداز | اهداف | مأموریت | راهبرد | اقدامات | ساختار |
|---|---|---|---|---|---|---|
| امریکا ( Cyber Security Strategy for Defence, 2014) | ارتباط میان چشم‌انداز و ارزش‌ها تصریح‌شده است. | اهداف آفندی نیز ذکر شده است. | توجه به پدافند غیرعامل | توجه به نخبه‌پروری از سوی وزارت دفاع در حوزه سایبری | شاخص‌گذاری سلامت فضای سایبر- ایجاد شبکه ملی هشدار | دفاع سایبری زیر نظر ارتش و برخی هم در حیطه امنیت داخلی- همکاری نزدیک دفاع و امنیت داخلی – وابسته بودن امنیت آمریکا به هوش مردم |
| انگلیس (UK Cyber Security Strategy, 2011) | توجه جدی به صنعت و اقتصاد برای امنیت ملی شده است. | توجه به امنیت فضای کسب‌وکار و عدم ذکر سیاست‌های دفاعی | | دولت نقش هماهنگی و همراهی راهبردها را دارد تا دخالت مستقیم | ایجاد یک مرجع برای آگاهی‌رسانی به مردم | |
| استرالیا ( Cyber Security, 2013 Strategy) | | توجه به نقش جدی مردم در ایجاد امنیت | رهبری قوی و مدیریت فضا در سطح ملی | | | حضور بخش خصوصی در ایجاد امنیت همراه با بخش‌های امنیتی |
| ترکیه ( Cyber Crime Threat Intelligence, 2014) | | | | رمزنگاری و ترویج آموزش‌ها از سطوح ابتدایی- کنترل واردات رمزنگاری | ارزیابی ریسک و تعیین تهدیدات توسط سازمان ملی امنیت اطلاعات- توجه و نظارت بر محتوا | |

| کشور | چشم‌انداز | اهداف | مأموریت | راهبرد | اقدامات | ساختار |
|---|---|---|---|---|---|---|
| کره جنوبی (Cyber Security Strategy Plan, 2013) | بهترین دولت دیجیتال در جهان و هماهنگ با کشورها | دفاع چندلایه: گیت وی، آی اس پی و کاربران | | فرهنگ‌سازی امنیت سایبری | | |
| رژیم صهیونیستی (The Future of Israel's Security, 2011) | عدم ذکر شفاف چشم‌انداز و دکترین | | | جذب سرمایه‌گذاری شرکت‌های خارجی فعال صنعت فاوا و افتا | مدیریت ریسک همکاری بین ارتش (نیروهای مسلح) و سازمان امنیتی و بخش خصوصی. | |
| اتحادیه اروپا Cybersecurity Strategy of the European Union,2013 | | | | ۱- کاهش شدید جرائم سایبری. ۲- رونق بازار صنعت افتا. ۳- ترویج تعامل و هماهنگی بین بازیگران بخش نظامی و غیرنظامی در اتحادیه با تأکید بر تبادل بهترین تجارب، تبادل اطلاعات و پیش‌آگاهی، پاسخ به تهدیدها، ارزیابی تهدید، بالا بردن آگاهی و محسوب کردن امنیت سایبر به‌عنوان یک اولویت | توسعه رمزنگاری ارتقاء استانداردهای راهنمای صنعت برای کیفیت عملکرد شرکت‌ها در امنیت سایبر و ارتقاء اطلاعات قابل دسترسی برای عموم، به‌وسیله توسعه برچسب‌های امنیتی یا نشانه‌های درجه‌بندی که به مصرف‌کننده در ارزیابی بازار کمک کند. | |

پس از بررسی اسناد بالادستی و مطالعات تطبیقی، گروه محققین گزاره‌های مورد نظر را از کلیدواژه‌های استخراج‌شده احصاء و در سلول‌های چارچوب معماری وارد نمودند.

با توجه به اهمیت انتخاب چارچوب معماری برای تلفیق هدفمند گزاره‌های استخراج‌شده از اسناد بالادستی و همچنین مطالعات تطبیقی، در ادامه مبحث به این موضوع می‌پردازیم:

**بهره‌گیری از چارچوب‌های معماری**

چارچوب‌های معماری مجموعه‌ای از مفاهیم، مدل‌ها، ابزارها و متدولوژی‌ها هستند که استراتژیست‌ها، معماران، طراحان و مجریان برنامه‌های سازمانی را قادر می‌سازند تا در کنار یکدیگر به طراحی و توسعه یکپارچه سازمان بپردازند. چارچوب‌های معماری سازمانی در عمل به‌صورت انتزاعی بوده و در حالت منفرد کاربرد علمی ندارند. لیکن این چارچوب‌ها تصویر یکپارچه‌ای از سازمان و اجزای اصلی آن را ارائه می‌نمایند. با استفاده از این چارچوب‌ها، لایه به لایه می‌توان سازمان را طراحی نمود؛ یعنی در بالاترین سطح آن (لایه راهبردی) فرایندهای سازمان قابل طراحی‌اند و محصول لایه‌های زیرین، سامانه‌های یکپارچه در سازمان هستند. هر چارچوب شامل یکسری ابزار و تعاریف است. هر چارچوب باید شامل یکسری استانداردها و محصولات آماده باشد که برای اجرای اجزای طراحی مورد استفاده قرار می‌گیرند. به‌عبارت‌دیگر چارچوب‌ها به‌مثابه یک جعبه‌ابزار و راهنما برای ساختن سازمان می‌باشند. برای اینکه بتوان قدم‌به‌قدم به ساختن سازمان پرداخت، باید از یکسری متدولوژی‌ها پیروی نمود تا سازمان شکل واقعی خود را بگیرد. متدولوژی‌ها روش‌های قدم‌به‌قدم استفاده از چارچوب‌ها هستند.

تاکنون چارچوب‌های مختلفی برای معماری سازمانی ارائه شده است. هریک از این چارچوب‌ها از دیدگاهی خاص و برای نوع خاصی از سازمان‌ها ارائه شده‌اند. مهم‌ترین

چارچوب‌هایی که تاکنون ارائه شده و توسعه یافته‌اند عبارت‌انـد از: چـارچوب زکمـن[۱]، برای سازمان‌های دولتی و خصوصی، چارچوب معماریFEAF[۲]، برای سازمان‌های دولتی ایـالات‌متحـده آمریکـا، چـارچوب معمـاریC4ISR/DoDAF[۳]، بـرای محـیط نظـامی ایالات‌متحده آمریکـا، چـارچوب معمـاریTEAF[۴]، بـرای وزارت دارایـی ایـالات‌متحـده آمریکا، چارچوب معماریTOGAF[۵]. بررسی‌ها نشان می‌دهد کـه نسـخه ۲,۲ چـارچوب DODAF، یکی از جامع‌ترین چارچوب‌های معماری مـی‌باشـد کـه بـرای وزارت دفـاع آمریکا بومی‌سازی شده است. درصورتی‌که بخواهیم برای طراحی نظام دفاع سایبری از چارچوب‌های معماری استفاده نماییم، در مرحله نخسـت مـی‌بایسـت ایـن چـارچوب بومی‌سازی شود که خود مستلزم یک پژوهش دیگر است، لذا به علت سادگی، جامعیت و در دسترس بودن مستندات و از طرف دیگر پوشش دادن تمـام خصوصـیاتی کـه در صفحات قبل به آن اشاره شد، گروه محققین تصمیم گرفت از چارچوب زکمن استفاده نماید. در این چارچوب برای دستیابی به یک ثبات نسبی به‌منظور طراحـی نظـام دفـاع سایبری در یک محیط سیال فضای سایبر، سطح راهبردی چارچوب زکمن انتخاب شـد و نظر به فرایند محور بودن این چـارچوب، در سـطح راهبـردی، سـتون‌هـای چطـور[۶] (فرایند) و چه کسی[۷] (نهاد) به‌عنوان محورهای اصلی گزینش و ستون‌های چرا[۸]، کـی[۹]، کجا[۱۰] و چه چیزی[۱۱]، ضمن احصـاء در پیوسـت پـژوهش، در سـتون فراینـد نگاشـت گردید.

1.Zachman
2. Federal EenterpriseAarchitecture Framework
3.Computers, Intelligence, Surveillance and Reconnaissance/ Department of Defense Architecture Framework
4.Treasury Enterprise Architecture Framework
5.The Open Group Architecture Framework
6.HOW
7.WHO
8.WHY
9.WHEN
10.WHERE
11.WHAT

**جدول (۴)**

| چه کسی؟ | چه چیز؟ | چطور؟ | کجا؟ | چه وقت؟ | چرا؟ |
|---|---|---|---|---|---|
| Who | What | How | Where | When | WHY |
| ساختار و نقش | موجودیت‌ها (هویت و اطلاعات) | فرایندها در لایه راهبرد | قلمرو | محرک‌ها | اهداف و راهبردها |

پس از تکمیل مطالعات صورت‌گرفته، کلیدواژه استخراج‌شده از اسناد بالادستی و همچنین کلیدواژه‌های حاصل از مطالعات تطبیقی پس از بومی‌سازی، توسط جمع خبرگی محققین، در سلول‌های چارچوب زکمن وارد گردید (به‌عبارت‌دیگر از کلیدواژه-های استخراج‌شده، گزاره‌هایی توسط گروه محققین تولید و در چارچوب زکمن وارد شد) و پس از تلفیق این گزاره‌ها تعداد ۱۸ فرایند به‌عنوان محصول اولیه سطح راهبردی این چارچوب تولید شد که جدول زیر آن را نشان می‌دهد:

**جدول (۵) فرایندها**

| فرایند | توصیف فرایند |
|---|---|
| F1 | برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هدایت فعالیت‌ها |
| F2 | آموزش، آگاه‌سازی و اطلاع‌رسانی |
| F3 | فرهنگ‌سازی امنیت سایبری |
| F4 | مدیریت همکاری و تعاملات داخلی و بین‌المللی |
| F5 | مدیریت مشارکت بخش خصوصی |
| F6 | بومی‌سازی در حوزه امنیت سایبر |
| F7 | رمزنگاری و امنیت اطلاعات متمرکز |
| F8 | ارتقاء خلاقیت، نوآوری، شکوفایی و ایجاد خودکفایی در حوزه امنیت سایبر |
| F9 | استانداردسازی در حوزه امنیت سایبر |
| F10 | نظارت و ارزیابی مستمر، حفظ و ارتقاء آمادگی بخش‌های مختلف نظام دفاع سایبری |
| F11 | ایجاد بازدارندگی و پیشگیری از حملات و تهدیدات |
| F12 | ارزیابی مخاطرات و تهدیدات سایبری و به‌روزرسانی آن‌ها |
| F13 | پیگیری مؤثر قانونی و حقوقی جرائم و حملات سایبری |
| F14 | پایش، رصد مستمر تهدیدات و تشخیص حملات |
| F15 | پاسخ، مقابله سریع و مؤثر با تهدیدات و حملات سایبری |
| F16 | مدیریت مخاطرات و حوادث |
| F17 | تقویت پایداری در مقابل حملات |
| F18 | بازیابی و مدیریت بحران |

در ادامه مراحل پژوهش به تشریح نحوه سطح‌بندی این فرایندها و همچنین برقراری روابط بین آن‌ها برای ایجاد یکپارچگی در دفاع سایبری می‌پردازیم.

## روش‌شناسی تحقیق

پژوهش حاضر از لحاظ نوع، توسعه‌ای و کاربردی بوده و روش به‌کارگیری‌شده در آن موردی-زمینه‌ای است؛ یعنی پژوهشگر پس از مطالعه موقعیت قبلی دفاع سایبری در کشور و بررسی وضعیت موجود، برای دستیابی به وضعیت مطلوب مبادرت به بررسی اسناد بالادستی و مطالعه تطبیقی سایر کشورها نموده و درنهایت مدل مفهومی وضعیت جدید را ارائه می‌نماید؛ بنابراین این شیوه، از مراحل پژوهش موردی-زمینه‌ای است. این روش، تصویری روشن و گسترده در موردی ویژه ارائه می‌کند و پژوهشگران تمام مواردی که در سرزمین‌های خاص مطرح است را مورد تجزیه‌وتحلیل قرار می‌دهند. روش پژوهش موردی- زمینه‌ای عبارت از مطالعه عمیق و ژرف‌نگر روی نمونه‌هایی از پدیده در محیط طبیعی است. تلاش می‌شود هرچه بیشتر متغیرهای ناخواسته کنترل شوند و متغیرهای مستقل بیشتری مورد بررسی قرار گیرند (خلیلی شورینی،۱۳۹۱: ۱۲۸).

جامعه آماری در این پژوهش عبارت از: متخصصین، پژوهشگران، مدیران و دست‌اندرکاران اجرایی که در حوزه فناوری اطلاعات و فضای سایبری کشور فعالیت می‌نمایند و از دانش راهبردی در این حوزه برخوردار هستند. برای دستیابی به حجم نمونه از نمونه‌گیری تصادفی ناحیه‌ای یا خوشه‌ای استفاده شده است. در تحقیقات کیفی نمونه‌گیری تا حد اشباع صورت می‌گیرد؛ اما توصیه شده است که در ابتدا حداقلی از تعداد نمونه در طرح تحقیق در نظر گرفته شود و به‌تدریج در حین انجام تحقیق احتمال افزایش این تعداد وجود دارد (Patton, 2002).

در این پژوهش با استفاده از اطلاعات گروه تحقیق، اسامی تعداد ۳۰ نفر از خبرگان حوزه‌های راهبردی فضای سایبر که با مباحث دفاعی آشنا بودند به‌صورت گلوله برفی گردآوری گردید، ولی به علت محدودیت‌های روش مورد استفاده؛ یعنی مدل‌سازی ساختاری تفسیری و مقایسه‌ای زوجی (ISM)، (حداکثر پرسشنامه مورد نیاز برای روش

ISM، ۱۴ پرسشنامه می‌باشد که مورد بهره‌برداری قرار گرفت)؛ تعداد چهارده نفر از آن‌ها گزینش و به‌صورت مکرر با مصاحبه فردی و جمعی و تشکیل جلسات طوفان فکری، به آن‌ها رجوع گردید.

در این پژوهش تلاش شده است برای گردآوری اطلاعات از روش کتابخانه علمی و تخصصی، سایت‌های معتبر اینترنتی، همچنین روش میدانی شامل مصاحبه (فردی و جمعی) با خبرگان فضای سایبر، فناوری اطلاعات و ارتباطات به‌صورت مکرر بهره‌برداری شود؛ مانند:

الف: برای دستیابی به وضعیت موجود کشور در دفاع سایبری پس از گردآوری اطلاعات لازم، جلسه طوفان فکری با حضور خبرگان موصوف برگزار شد و نقشه وضعیت موجود ترسیم گردید؛

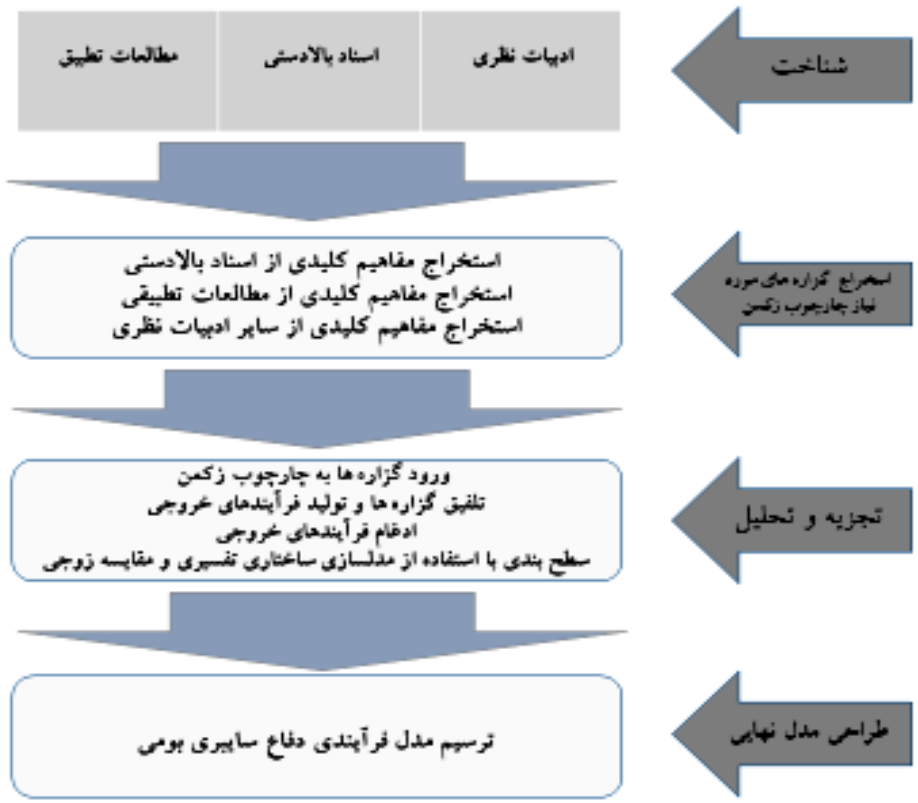
ب: پس از استخراج کلمات کلیدی از اسناد بالادستی و مطالعات تطبیقی برای تبدیل آن‌ها به گزاره و ورود در چارچوب زکمن دوباره جلسه گروهی خبرگان به‌صورت متوالی برگزار گردید؛

ج: با توجه به پیچیده بودن پرسشنامه روش ISM جلسه با آن‌ها برگزار و پس از تنظیم پرسشنامه و بررسی روایی پرسشنامه نحوه تکمیل آن نیز تشریح گردید؛

د: ادغام فرایندهای حاصل از چارچوب زکمن نیز در جلسه گروه خبرگان صورت پذیرفت (ادغام ۱۸ فرایند و تبدیل آن به ۱۲ فرایند)؛

ه: نام‌گذاری مراحل مختلف فرایند اصلی نیز خروجی کارگروهی خبرگان بوده است.

گفتنی است پرسش‌نامه ابزار دیگری بود که در این زمینه مورد استفاده قرار گرفت. نقشه راه پژوهش به‌طور اجمال به شرح ذیل می‌باشد:




**شکل (۱) نقشه راه پژوهش**

## تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

برای انجام این پژوهش از روش مدل‌سازی ساختاری تفسیری و مقایسه‌ای زوجی (ISM) استفاده شده است. در مرحله نخست قبل از تجزیه‌وتحلیل داده‌های حاصل از پژوهش بر اساس محدودیت‌ها و الزامات مدل‌سازی ساختاری تفسیری و مقایسه‌ای زوجی، ۱۸ فرایند حاصل از چارچوب معماری زکمن با کسب نظر خبرگان (برگزاری جلسه و مصاحبه با خبرگان حوزه پژوهش) ادغام شد و به ۱۲ فرایند تبدیل گردید که در جدول ذیل نشان داده شده است:

**جدول (۶): فرایندهای نهایی پس از ادغام**

| فرایند | توصیف فرایند |
|---|---|
| F1 | برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هدایت فعالیت‌ها |
| F2 | فرهنگ‌سازی، آموزش، آگاه‌سازی و اطلاع‌رسانی |
| F3 | مدیریت همکاری و تعاملات بین‌المللی |
| F4 | مدیریت مشارکت بخش خصوصی |
| F5 | بومی‌سازی، استانداردسازی، نوآوری و ایجاد خودکفایی |
| F6 | رمزنگاری |
| F7 | نظارت و ارزیابی |
| F8 | ایجاد بازدارندگی و پیشگیری از تهدیدات و حملات سایبری |
| F9 | پیگیری حقوقی جرائم و حملات سایبری |
| F10 | پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری |
| F11 | مدیریت مخاطرات و ارتقاء آمادگی و پایداری در مقابل حملات سایبری |
| F12 | بازیابی و مدیریت بحران |

این روش یک فرآیند یادگیری تعاملی است که در آن مجموعه‌هایی از عناصر مختلف و به‌هم‌مرتبط در یک مدل نظام‌مند جامع ساختاردهی می‌شوند. این روش‌شناسی به ایجاد و جهت دادن به روابط پیچیده میان عناصر یک سیستم کمک می‌نماید. یکی از اصلی‌ترین منطق‌های این روش آن است که همواره عناصری که در یک سیستم اثرگذاری بیشتری بر سایر عناصر دارند از اهمیت بالاتری برخوردارند. مدلی که با استفاده از این متدولوژی به دست می‌آید، ساختاری از یک مسئله یا موضوع پیچیده، یک سیستم یا حوزه مطالعاتی را نشان می‌دهد که الگویی به‌دقت طراحی‌شده است؛ درنتیجه، می‌توانیم بگوییم که مدل‌سازی ساختاری تفسیری، نه‌تنها بینشی را در خصوص روابط میان عناصر مختلف یک سیستم فراهم می‌نماید، بلکه ساختاری را مبتنی بر اهمیت و یا تأثیرگذاری عناصر برهم‌بسته به نوع رابطه محتوایی تعریف‌شده فراهم می‌نماید و نمایشی تصویری از آن را ارائه می‌دهد. این روش یک فن مدل‌سازی است که روابط مشخص و ساختار کلی در یک مدل دیاگرام، نشان داده می‌شود. ایده اصلی مدل‌سازی ساختاری

تفسیری تجزیه یک سیستم پیچیده به چند زیرسیستم عناصر با استفاده از تجربه عملی و دانش خبرگان به‌منظور ساخت یک مدل ساختاری چندسطحی است. مراحل تجزیه‌وتحلیل در این روش به شرح ذیل می‌باشد:

- تعیین متغیرها یا معیارها: به دست آوردن ماتریس ساختار روابط درونی متغیرها یا معیارها (خودتعاملی ساختاری) که از طریق نظرسنجی حاصل می‌شود. در سطر و ستون اول این ماتریس، متغیرها به ترتیب ذکر می‌شوند. آنگاه روابط دوبه‌دوی متغیرها توسط نمادهایی مشخص می‌شوند. در مرحله اول روابط و سطح تأثیرگذاری تک‌تک فرایندها بر روی هم سنجیده می‌شود؛ بنابراین یک ماتریس ۱۲*۱۲ از فرایندها تشکیل می‌گردد (به‌منظور اخذ سریع‌تر نظرات به‌صورت بالا مثلثی)، نظر خبرگان در ارتباطات چهارگانه (V,A,X,O) اخذ می‌شود.

**جدول (۷) ماتریس خودتعاملی**

| اگر سطر روی ستون تاثیر داشته باشد - V<br>اگر ستون روی سطر تاثیر داشته باشد - A<br>اثر متقابل - X<br>بی اثر - O | فرآیند | برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت فعالیتها | فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | همکاری و تعاملات بین المللی | مشارکت بخش های دولتی و خصوصی | بومی سازی، استاندارد سازی ، نوآوری و ایجاد خود کفایی | ایجاد رمزنگاری و امنیت اطلاعات متمرکز | نظارت و ارزیابی | ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | بازیابی و مدیریت بحران |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | F۱ | F۲ | F۳ | F۴ | F۵ | F۶ | F۷ | F۸ | F۹ | F۱۰ | F۱۱ | F۱۲ |
| برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت فعالیتها | F۱ | | x | v | v | v | v | v | v | v | a | x | v |
| فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | F۲ | | | x | v | v | v | a | x | o | x | x | x |
| همکاری و تعاملات بین المللی | F۳ | | | | x | v | a | a | v | v | x | v | v |
| مشارکت بخش های دولتی و خصوصی | F۴ | | | | | v | v | a | v | o | v | v | v |
| بومی سازی، استاندارد سازی ، نوآوری و ایجاد خود کفایی | F۵ | | | | | | v | a | v | v | v | v | v |
| ایجاد رمزنگاری و امنیت اطلاعات متمرکز | F۶ | | | | | | | a | v | o | o | v | o |
| نظارت وارزیابی | F۷ | | | | | | | | v | v | v | v | v |
| ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | F۸ | | | | | | | | | a | a | a | v |
| پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | F۹ | | | | | | | | | | v | | a |
| پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | F۱۰ | | | | | | | | | | | v | a |
| حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | F۱۱ | | | | | | | | | | | | a |
| بازیابی و مدیریت بحران | F۱۲ | | | | | | | | | | | | |

- **به دست آوردن ماتریس دستیابی:** طبق توصیه‌های روش ISM لازم است که در مرحله بعد، نظرات اخذشده با استفاده از اعداد صفر (فاقد تأثیرگذاری) و یک (تأثیرگذار) به کل ماتریس بسط داده شود.

**جدول (۸): ماتریس دستیابی**

| تاثیرگذاری - ۱<br>عدم تاثیرگذاری - ۰ | فرآیند | برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت | فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | همکاری و تعاملات بین المللی | مشارکت بخش های دولتی و خصوصی | بومی سازی، استاندارد سازی، نوآوری و ایجاد خود کفایی | ایجاد رمزنگاری و امنیت اطلاعات متمرکز | نظارت وارزیابی | ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | بازیابی و مدیریت بحران |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **فرآیند** | | F۱ | F۲ | F۳ | F۴ | F۵ | F۶ | F۷ | F۸ | F۹ | F۱۰ | F۱۱ | F۱۲ |
| برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت فعالیتها | F۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۰ | ۱ | ۱ |
| فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | F۲ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ |
| همکاری و تعاملات بین المللی | F۳ | ۰ | ۱ | ۱ | ۱ | ۱ | ۰ | ۰ | ۱ | ۱ | ۱ | ۱ | ۱ |
| مشارکت بخش های دولتی و خصوصی | F۴ | ۰ | ۰ | ۱ | ۱ | ۱ | ۱ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ |
| بومی سازی، استاندارد سازی، نوآوری و ایجاد خود کفایی | F۵ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۰ | ۱ | ۱ | ۱ | ۱ | ۱ |
| ایجاد رمزنگاری و امنیت اطلاعات متمرکز | F۶ | ۰ | ۰ | ۱ | ۰ | ۰ | ۱ | ۰ | ۱ | ۰ | ۰ | ۱ | ۰ |
| نظارت وارزیابی | F۷ | ۰ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ |
| ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | F۸ | ۰ | ۱ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ |
| پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | F۹ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۱ | ۰ | ۰ |
| پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | F۱۰ | ۱ | ۱ | ۱ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۱ | ۱ | ۰ |
| حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | F۱۱ | ۱ | ۱ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۰ | ۱ | ۰ |
| بازیابی و مدیریت بحران | F۱۲ | ۰ | ۱ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۱ | ۱ |

- **سازگار کردن ماتریس دستیابی (سازگاری درونی):** در این مرحله، ماتریسی از حاصل جمع کلیه سلول‌های همسان ماتریس‌های دستیابی اخذشده از کلیه پرسشنامه‌ها تنظیم می‌نماییم.

**جدول (۹): ماتریس حاصل جمع**

| حاصل جمع | فرآیند | برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت | فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | همکاری و تعاملات بین المللی | مشارکت بخش های دولتی و خصوصی | بومی سازی، استاندارد سازی ،نوآوری و ایجاد خود کفایی | ایجاد رمزنگاری و امنیت اطلاعات متمرکز | نظارت و ارزیابی | ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | بازیابی و مدیریت بحران |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **فرآیند** | | F۱ | F۲ | F۳ | F۴ | F۵ | F۶ | F۷ | F۸ | F۹ | F۱۰ | F۱۱ | F۱۲ |
| برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت فعالیتها | F۱ | ۱۰ | ۱۰ | ۹ | ۱۰ | ۱۰ | ۱۰ | ۷ | ۱۰ | ۹ | ۸ | ۱۰ | ۱۰ |
| فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | F۲ | ۶ | ۱۰ | ۶ | ۷ | ۸ | ۷ | ۵ | ۸ | ۴ | ۷ | ۸ | ۸ |
| همکاری و تعاملات بین المللی | F۳ | ۳ | ۵ | ۱۰ | ۴ | ۵ | ۵ | ۲ | ۸ | ۹ | ۸ | ۷ | ۸ |
| مشارکت بخش های دولتی و خصوصی | F۴ | ۴ | ۳ | ۵ | ۱۰ | ۱۰ | ۹ | ۴ | ۹ | ۵ | ۹ | ۹ | ۹ |
| بومی سازی، استاندارد سازی ، نوآوری و ایجاد خود کفایی | F۵ | ۲ | ۳ | ۳ | ۳ | ۱۰ | ۹ | ۳ | ۹ | ۴ | ۸ | ۹ | ۹ |
| ایجاد رمزنگاری و امنیت اطلاعات متمرکز | F۶ | ۲ | ۴ | ۵ | ۳ | ۳ | ۱۰ | ۱ | ۹ | ۳ | ۵ | ۱۰ | ۴ |
| نظارت وارزیابی | F۷ | ۳ | ۵ | ۳ | ۳ | ۲ | ۴ | ۱۰ | ۹ | ۵ | ۹ | ۹ | ۸ |
| ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | F۸ | ۲ | ۴ | ۳ | ۳ | ۴ | ۳ | ۱ | ۱۰ | ۴ | ۷ | ۷ | ۷ |
| پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | F۹ | ۲ | ۳ | ۵ | ۳ | ۰ | ۱ | ۱ | ۷ | ۱۰ | ۳ | ۲ | ۴ |
| پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | F۱۰ | ۴ | ۴ | ۴ | ۳ | ۴ | ۱ | ۲ | ۸ | ۴ | ۱۰ | ۸ | ۵ |
| حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | F۱۱ | ۴ | ۴ | ۴ | ۴ | ۳ | ۴ | ۱ | ۶ | ۴ | ۴ | ۱۰ | ۷ |
| بازیابی و مدیریت بحران | F۱۲ | ۲ | ۵ | ۳ | ۳ | ۴ | ۱ | ۱ | ۴ | ۲ | ۳ | ۴ | ۱۰ |

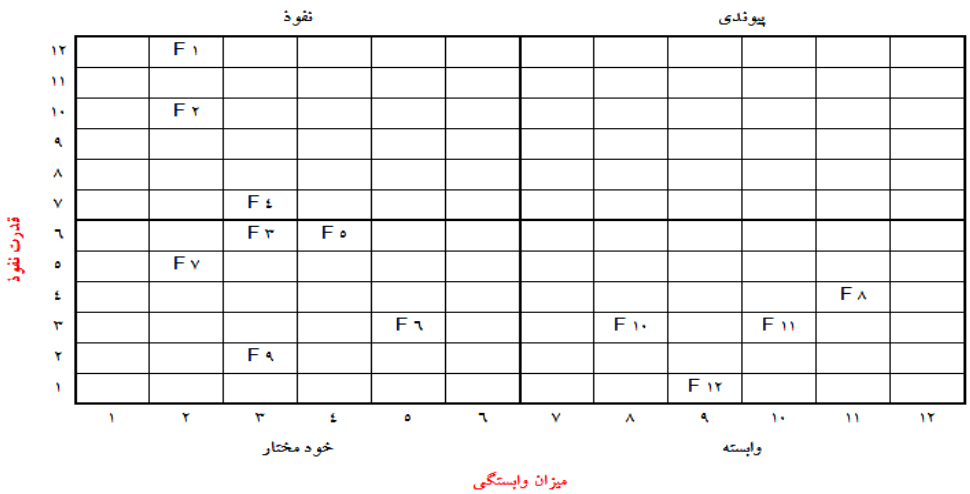
**تجزیه‌وتحلیل MICMAC**: پس از دستیابی به ماتریس مجموع پرسشنامه‌ها، درصورتی‌که مقادیر هر سلول یک تا پنج باشد با عدد صفر و اگر بیشتر از پنج باشد با عدد یک جایگزین می‌گردد و سپس حاصل جمع سطر و ستون محاسبه می‌گردد که در ماتریس ذیل نشان داده شده است.

**جدول (۱۰): ماتریس دستیابی نهایی**

| بزرگتر از ۵ - ۱<br>کوچکتر یا مساوی با ۵ - ۰ | فرآیند | برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت | فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | همکاری و تعاملات بین المللی | مشارکت بخش های دولتی و خصوصی | بومی سازی، استاندارد سازی ،نوآوری و ایجاد خود کفایی | ایجاد رمزنگاری و امنیت اطلاعات متمرکز | نظارت و ارزیابی | ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | بازیابی و مدیریت بحران | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **فرآیند** | | F۱ | F۲ | F۳ | F۴ | F۵ | F۶ | F۷ | F۸ | F۹ | F۱۰ | F۱۱ | F۱۲ | |
| برنامه ریزی، هماهنگی، یکپارچه سازی، همزمان سازی و هدایت فعالیتها | F۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱۲ |
| فرهنگ سازی، آموزش، آگاه سازی و اطلاع رسانی | F۲ | ۱ | ۱ | ۱ | ۱ | ۱ | ۱ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ | ۱۰ |
| همکاری و تعاملات بین المللی | F۳ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۱ | ۱ | ۱ | ۶ |
| مشارکت بخش های دولتی و خصوصی | F۴ | ۰ | ۰ | ۰ | ۱ | ۱ | ۱ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ | ۷ |
| بومی سازی، استاندارد سازی ، نوآوری و ایجاد خود کفایی | F۵ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ | ۶ |
| ایجاد رمزنگاری و امنیت اطلاعات متمرکز | F۶ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۱ | ۰ | ۰ | ۱ | ۰ | ۳ |
| نظارت وارزیابی | F۷ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۰ | ۱ | ۱ | ۱ | ۵ |
| ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری | F۸ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۱ | ۱ | ۱ | ۴ |
| پیگیری موثر قانونی و حقوقی جرایم و حملات سایبری | F۹ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ | ۰ | ۰ | ۰ | ۲ |
| پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری | F۱۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۱ | ۱ | ۰ | ۳ |
| حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری | F۱۱ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۱ | ۱ | ۳ |
| بازیابی و مدیریت بحران | F۱۲ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۱ | ۱ |
| | | ۲ | ۲ | ۳ | ۳ | ۴ | ۵ | ۲ | ۱۱ | ۳ | ۸ | ۱۰ | ۹ | |

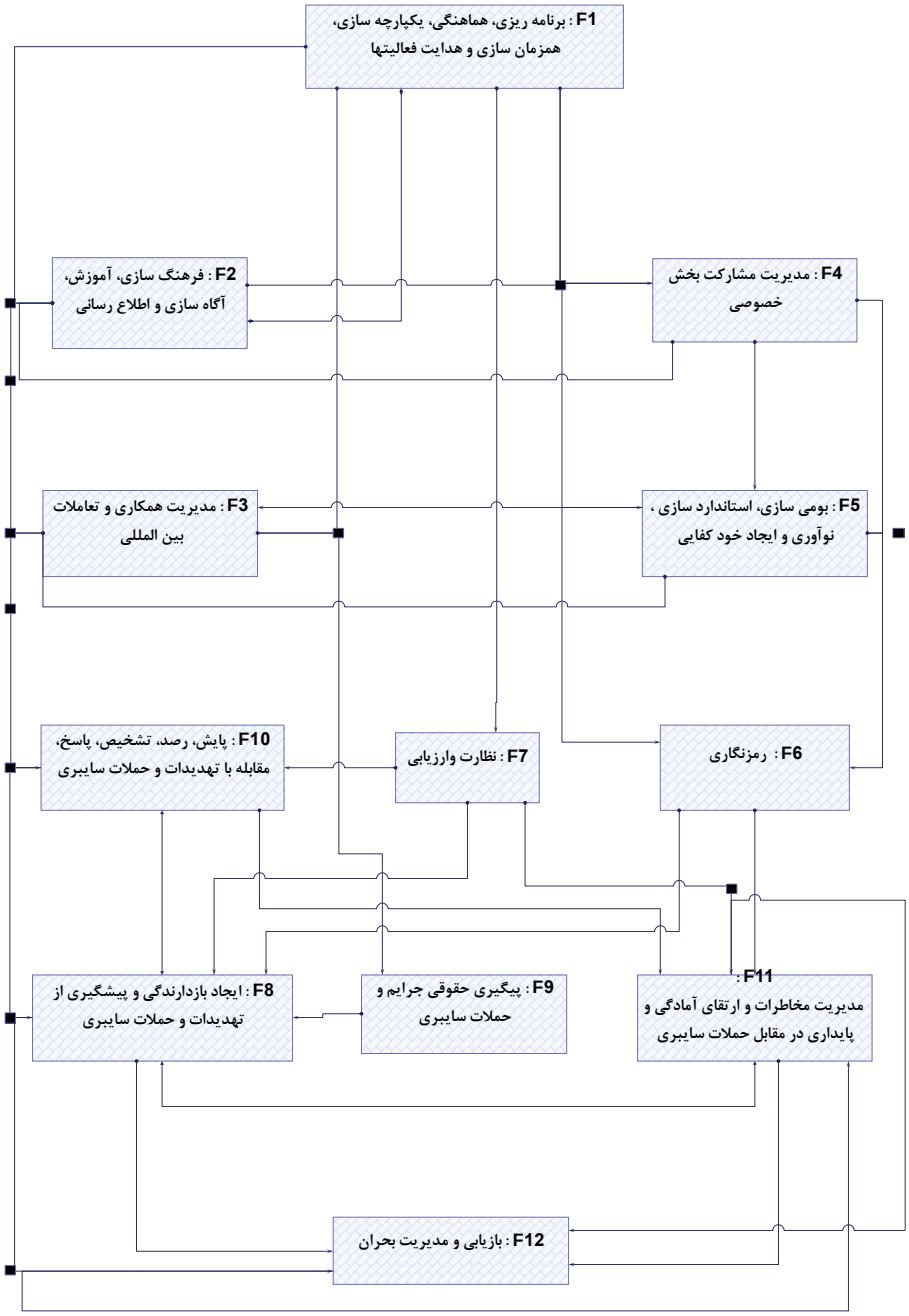
با استفاده از ماتریس تعیین موقعیت، موقعیت هریک از فرایندها در چهار وضعیت پیوندی، نفوذ، خودمختار و وابسته تعیین می‌گردد.

**جدول (۱۱): موقعیت هریک از فرایندها در چهار وضعیت پیوندی، نفوذ، خودمختار، وابسته**




### سطح‌بندی فرایندها و تعیین ورودی و خروجی

در این مرحله ورودی و خروجی هریک از فرایندها و سپس نقاط مشترک آن‌ها مورد محاسبه قرار گرفته و درنهایت با استفاده از نقاط مشترک، سطح این فرایندها تعیین و در شش سطح به‌صورت سلسله‌مراتبی تدوین گردید که برای هر لایه می‌توان نام مناسبی را اختصاص داد. درنهایت مدل فرایندی دفاع سایبری به شرح ذیل ارائه گردید:




**شکل (۲) مدل فرایندی دفاع سایبری**

## نتیجه‌گیری

در مبحث نتیجه‌گیری، به سؤال‌های پژوهش پاسخ داده می‌شود؛ در این پژوهش نیز نخست اسناد بالادستی کشور، برای پاسخ به سؤال‌های فرعی پژوهش؛ یعنی «اسناد بالادستی در این زمینه کدامند؟» شناسایی گردید و سپس مطالعات تطبیقی در پاسخ به سؤال فرعی «ارکان جهت‌ساز و راهبردهای دفاع سایبری کشورهای مورد مطالعه چگونه است؟» صورت گرفت و با استخراج گزاره‌های اصلی از این منابع توسط گروه خبرگی، نتایج در چارچوب زکمن وارد و محصول نهایی آن؛ یعنی فرایندهای ۱۸ گانه، دوباره توسط گروه خبرگی تلخیص و با استفاده از روش مدل‌سازی ساختاری تفسیری و مقایسه‌ای زوجی، مدل فرایندی نهایی ارائه شده است که در راستای پاسخ به سؤال اصلی پژوهش؛ یعنی «فرایندهای اصلی دفاع سایبری بومی کشور کدامند؟» قرار دارد. همان‌گونه که در مدل ترسیم‌شده مشاهده می‌شود، این مدل شامل دوازده فرایند اصلی می‌باشد؛ ورودی‌ها و خروجی‌های هر فرایند در این مدل نشان داده شده است؛ به‌طوری‌که خروجی برخی از فرایندها به‌عنوان ورودی فرایند دیگر محسوب گردیده و در مجموع به‌صورت هدفمند دفاع سایبری بومی و یکپارچه را پایه‌ریزی می‌نمایند. در این مدل سطوح گوناگونی مشاهده می‌شود که هریک از این لایه‌ها را می‌توان به تناسب فرایندهای موجود در آن، نام‌گذاری نمود.

## پیشنهاد

۱. با بهره‌گیری از نگاشت نهادی یا سایر روش‌های مرسوم، متولیان هریک از فرایندهای دفاع سایبری استخراج، نقش و شرح وظایف آن‌ها تبیین و راهبردهای اجرای آن تدوین گردد.
۲. با توجه به اینکه چارچوب‌های مورد استفاده در سطح جهان به‌طور کامل از ارزش‌های اسلامی و مبانی جمهوری اسلامی ایران پشتیبانی نمی‌نمایند، چارچوب معماری بومی برای کشور توسعه داده شود.
۳. نظام دفاع سایبری کشور با چارچوب بومی تدوین گردد.

# فهرست منابع ومآخذ

## الف. منابع فارسی


- قرآن کریم
- نهج‌البلاغه
- اصلانی مقدم، مصطفی (۱۳۸۵)، جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی ج.ا.ا، دکتری، دانشگاه عالی دفاع ملی، بازیابی از ۱۰.
- امیدوارنیا، محمدجواد (۱۳۸۲)، امنیت در قرن بیست و یکم (دیدگاه چین)، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- امیرکبیری، علیرضا (۱۳۸۰)، مدیریت استراتژیک، نگاه دانش.
- بوزان، باری (۱۳۷۸)، مردم، دولت‌ها، هراس، پژوهشکده مطالعات راهبردی.
- پارساییان، علی و اعرابی، سید محمد (۱۳۹۴)، مدیریت استراتژیک، دفتر پژوهش‌های فرهنگی.
- جبار رشیدی، علی؛ نقیان فشارکی، مهدی و داداش تبار احمدی، کوروش (۱۳۹۲)، ارائه الگویی برای دفاع سایبری در آستانه حمله مبتنی بر پردازش رویدادهای پیچیده، ارائه‌شده در ششمین همایش فرامنطقه‌ای پیشرفت‌های نوین در علوم مهندسی.
- خلیلی شورینی، سیاوش (۱۳۹۱)، روش‌های پژوهش آمیخته، تهران: مؤسسه آموزشی یادواره کتاب، چاپ دوم.
- دهخدا، علی‌اکبر (۱۳۷۷)، لغت‌نامه دهخدا، (ج ۱۴)، تهران: مؤسسه انتشارات و چاپ دانشگاه تهران.
- رامک، مهراب؛ امیرلی، حسین؛ قربانی، ولی‌الله؛ حقی، مجید؛ کاظمی، موسی؛ رمضان یارندی، محسن؛ اسماعیلی، علی؛ یزدانی، سعید و ملائی، علی (۱۳۹۵)، طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، رساله گروهی، دانشگاه عالی دفع ملی، دانشکده امنیت.
- شرکت اندیشه پردازان شریف (۱۳۸۵)، الزامات جنگ‌های نوین در فضای سایبر (مجازی)، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فناوری دفاعی.
- شمس، فریدون (۱۳۸۳)، مفاهیم پایه معماری سازمانی، ماهنامه توسعه و کاربری فناوری ارتباطات و اطلاعات (تکفا)، سال دوم، شماره ۳.
- معین، محمد (۱۳۸۲)، فرهنگ معین، تهران: انتشارات امیرکبیر.
- موسوی الخمینی، سید روح‌الله (۱۳۸۹)، صحیفه امام، ج ۱۶ و ۲۱، تهران: مؤسسه تنظیم و نشر آثار امام خمینی (ره).

- قاضی نوری، سید سپهر و قاضی نوری، سید سروش (۱۳۸۷)، استخراج راهکارهای اصلاح نظام ملی نوآوری ایران با تکیه بر مطالعه تطبیقی کشورهای منتخب، سیاست علم و فناوری، ۱(۱)، ۶۴.
- گروه پدافند غیرعامل وزارت دفاع (۱۳۸۷)، تهدیدات شبکه‌ای، تهران: وزارت دفاع و پشتیبانی نیروهای مسلح، مؤسسه آموزشی و پژوهشی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فناوری دفاعی.
- مرآتی (۲۰۰۹)، تدوین روش توسعه چارچوب‌های معماری سازمان‌های دفاعی، مجله سیاست دفاعی، ۲۰(۷۹).
- مرآتی، احسان (۱۳۹۱)، تدوین روش توسعه چارچوب‌های معماری سازمان‌های دفاعی، سیاست دفاعی، ۳(۲۰)، ۶۰–۳۳.
- مؤسسه آموزشی و تحقیقاتی صنایع دفاع (۱۳۹۰)، راهبردهای امنیت فضای سایبری در سه کشور انگلستان، آلمان و آمریکا، مؤسسه آموزشی و تحقیقاتی صنایع دفاع.
- نادری خورشیدی، علی‌رضا؛ فقیه‌علی‌آبادی، هادی و میرعباسی، رمضان (۱۳۹۱)، معماری سازمانی زمینه‌ساز استقرار و توسعه معماری اطلاعات در دستگاه‌های دفاعی و اجرایی کشور، سیاست دفاعی، ۳(۲۰)، ۹۶–۶۱.


## ب. منابع انگلیسی


- ACST–Strategy-CyberSecurity., (2014), Cyber Security Strategy for Defence, ACST–Strategy CyberSecurity.
- Beggs, P., (2010), Securing the Nation’s Critical Cyber Infrastructure. US Department Of Homeland Security, Retrieved from -
- http://www.ocio.ca.gov/OIS/Government/events/documents/Patrick_Beggs.pdf
- Cheetancheri, S. G., (2004), Automated Reasoning in Co-operative Cyber Defense-A PhD thesis proposal.
- Commonwealth of australia., (2009), Cyber Security Strategy, australian government.
- Crown., (2011), UK Cyber Security Strategy.pdf. Crown copyright.
- Dogrul, M., Aslan, A. & Celik, E., (2011), Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. In Cyber conflict (ICCC), 2011 3rd international conference on (pp. 1–15). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5954698
- EUROPEAN COMMISSION., (2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, EUROPEAN COMMISSION.
- Even, S. & Ţov, D. S., (2012), Cyber Warfare: Concepts and Strategic Trends, Institute for National Security Studies.
- Federal Ministry of the Interior., (2011), Cyber Security Strategy for Germany, Federal Ministry of the Interior.
- Frei, S., (2014), Cyber Crime Threat Intelligence – Turkey, CSIS - Cyber Security Intelligence Service.

- Gelinas, R. R., (2010), Cyberdeterrence and the problem of attribution.
- Goodman, W., (2010), Cyber deterrence: Tougher in theory than in practice? DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528033
- Grafik, A., (2013), Austrian Cyber Security Strategy, Federal Chancellery of the Republic of AustriaCrown., (2011), UK Cyber Security Strategy.pdf. Crown copyright.
- Ik-kyoon, O., (2013), The National Cyber Security Strategy Plan | Korea IT Times, korea it times. Retrieved March 04, 2016, from.http://www.koreaittimes.com /story /31796/national-cyber-security-strategy-plan.
- ISO 9000 Introduction and Support Package., (2008), Guidance on the Concept and Use of the Process Approach for management systems.
- John D., (2012), Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress, Congressional Research Service US.
- Homeland Security., (2011), Blueprint for a Secure Cyber Future, Homeland Security.
- Ik-kyoon, O., (2013), The National Cyber Security Strategy Plan | Korea IT Times, korea it times. Retrieved March 04, 2016, from http://www.koreaittimes.com/story/31796/national-cyber-security-strategy-plan.
- Jenik, A., (2009), Cyberwar in Estonia and the Middle East, Network Security, 2009(4), 4–6.
- Kamal, A., (2005), The Law of Cyber-Space, An Invitation To The Table Of Negotiations, Published By United Nations Institute For Training And Research.
- Kirk Report., (2011), The Future of Israel's Security and the, U.S.-Israel Relationship.
- Kosina, K., (2012), Wargames in the fifth domain, Diplomatische Akademie.
- Leveson, N. G. (1995). Safeware: system safety and computers. ACM.
- Libicki, M. C., (2009), Cyberdeterrence and cyberwar, Santa Monica, Calif.: Rand.
- Luker, M. A., (2003), The national strategy to secure cyberspace, Educause Review, 38, 60–60.
- Park, T., (2009), Korean Cybersecurity Framework, ITU Regional Cybersecurity.
- Paxton, S. G., (2008), Enhanced cyberspace defense with real-time distributed systems using covert channel publish-subscribe broker pattern communications, Monterey California, Naval Postgraduate School.
- Ravi, (2005), Analysis of interactions among the barriers of reverse logistics, Technological Forecasting and Social Change. 72(8).
- Pramod, V. R. & Banwet, D. K., (2010), Interpretive structural modelling for understanding the inhibitors of a telecom service supply chain, IEOM (Dhaka, Bangladesh), 9–10, Retrieved from http://www.iieom.org/paper/Final Paper for PDF/101 Pramod Ram.pdf
- Stevens, G. M., (2003), Homeland Security Act of 2002: Critical Infrastructure Information Act, DTIC Document.
- Wong, T. P., (2011), Active cyber defense: enhancing national cyber defense.
- www.khamenei.ir.