دردست انتشار و غیر قابل انتشار

معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی– امنیتی

محمد رضا ولوی[۱]،حمیدرضا شجاع مودب[۲] حسین مددی آتشگاه[۳]

تاریخ دریافت: **تاریخ پذیرش:**

چکیده

برای مقابله با تهدیدات فضای سایبر در کشور، برنامه‌های راهبردی متعددی تدوین و ابلاغ شده است با این حال کشور گرفتار ضعف در تحقق اهداف کلان ملی در حوزه دفاعی-امنیتی در عرصه فضای سایبر می‌باشد زیرا فاقد معماری کلان هماهنگ و یکپارچه برای حاکمیت از جنبه دفاعی-امنیتی در عرصه فضای سایبر است بنابراین مسئله اصلی این تحقیق ارائه یک چنین معماری است. هدف از این مقاله ارائه معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی – امنیتی است و سئوال اصلی تحقیق این است که معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی– امنیتی چگونه است؟ روش تحقیق، کیفی است به اینصورت که ابتدا با مراجعه به مقالات و اسناد علمی سعی در پاسخگویی به سئوالات تحقیق شد، سپس با استفاده از روش گروه کانونی و با استفاده از معیارهای روایی و پایایی کیفی از جمله باورپذیری، انتقال‌پذیری، قابلیت اعتماد و تائیدپذیری نتایج مورد ارزیابی و تائید قرار گرفته است. بر اساس نتایج این تحقیق کشور برای تحقق اهداف کلان ملی خود از منظر دفاعی-امنیتی در عرصه فضای سایبر نیاز به پنج برنامه راهبردی پدافندی، آفندی، اطلاعاتی، صیانتی و توانمندسازی دارد که الزامات و نیازمندهای هر یک از برنامه‌های مذکور در این معماری ارائه شده است.

کلیدواژه‌ها: دفاعی-امنیتی، فضای سایبر، معماری، معماری کلان

[۱] دانشیار دانشگاه مالک اشتر و نویسنده مسئول:valavi@mut.ac.ir

[۲] دکتری مدیریت راهبردی دانشگاه عالی دفاع ملی hr.shoja2@sndu.ac.ir

[۳] دانشجوی دکتری مدیریت راهبردی دانشگاه عالی دفاع ملی h.m2adadi@sndu.ac.ir

۱. مقدمه:

با عنایت به ظهور، گسترش و تنوع تهدیدات سایبری که امروزه وجود دارد، لازم است مولفه‌های عینی و سایبری حاکمیت در حوزه دفاعی-امنیتی بصورت یکپارچه و هماهنگ با این تهدیدات و تهدیدات عینی مقابله نمایند. لذا در این مقاله ما اقدام به طراحی معماری کلان حاکمیت ج.ا.ا از جنبه دفاعی-امنیتی با تمرکز بر عرصه نوظهور فضای سایبر نموده‌ایم. بدین منظور لازم است نقش‌ها و فرایندهای دفاعی و امنیتی ج.ا.ا ایران با اهداف و راهبردهای کلان ملی در حوزه‌های دفاعی-امنیتی بطور کلی و مرتبط با فضای سایبر بطور خاص همخوانی داشته باشد.

نکته مهمی که باید مورد توجه قرار گیرد این است که خروجی در معماری سازمانی عبارتست از طرح پیشنهادی برای پیاده‌سازی سیستم‌های اطلاعاتی پشتیبانی کننده از فرایندهای کسب و کار است. اما خروجی در معماری کلان حاکمیت از جنبه دفاعی-امنیتی، نظام‌های کلان ملی مبتنی بر فرایندهای مدل‌سازی شده در این معماری می‌باشد به گونه‌ای که هر یک از این نظام‌ها چارچوب اصلی اسناد راهبردی دفاعی-امنیتی کشور در عرصه فضای سایبر را معین نمایند و از این طریق ما به منظومه راهبردی دفاعی-امنیت ج.ا.ا در عرصه فضای سایبر برسیم.

بیان مسئله:

حاکمیت ج.ا.ا در تحقق اهداف کلان دفاعی-امنیتی در عرصه فضای سایبر دچار نوعی ضعف می‌باشد و این ضعف به گونه‌ای است که در مواردی از طرف مقام معظم رهبری با عبارت "رها بودن" فضای سایبر توصیف می‌شود. بررسی‌ها نشان می‌هد که این ضعف ناشی از مسائلی است که در برنامه‌های راهبردی کشور در حوزه دفاعی-امنیتی فضای سایبر وجود دارند و اصلی‌ترین آنها این است که فضای سایبر از جنبه دفاعی-امنیتی یک موضوع بسیار پیچیده است که عدم احصاء، توازن و تناسب بین مولفه‌های اصلی آن و ابهام در کیفیت ارتباط آنها منجر به ضعف تحقق اهداف کلان ملی شده است. به عبارت دیگر کشور به این دلیل از عدم تحقق اهداف کلان ملی در این حوزه رنج می‌برد که فاقد معماری کلان هماهنگ و یکپارچه برای حاکمیت از جنبه دفاعی-امنیتی در عرصه فضای سایبر است به گونه‌ای که بتواند ارتباط بین اهداف و راهبردهای کلان ملی با ماموریت‌ها و اهداف دفاعی-امنیتی فضای سایبر و فرایندهای دفاعی-امنیتی و نقش‌های مرتبط با این حوزه برقرار نماید(**منبع:مطالعه گروهی داامنیت - داعا، ۱۴۰۰: ۴**) و از این جهت فقدان یک معماری کلان فضای سایبر با رویکرد دفاعی-امنیتی عملاً تبدیل به حلقه مفقوده بین اهداف کلان ملی با تحقق عملیاتی آنها شده است و همین باعث ضعف حاکمیت در تحقق اهداف مذکور گردیده است. لذا مسئله اصلی این تحقیق ارائه یک چنین معماری است.

اهمیت تحقیق:

۱- با توجه به تأکید مستقیم مقام معظم رهبری بر ضرورت ارتقاء قدرت سایبری ج.ا.ا در تراز جهانی در بند ۳ حکم ابلاغی سیاست‌های فضای مجازی سال ۹۴، معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی –

امنیتی در جهت برآورده کردن منویات معظم له امری مهم و اساسی است.

۲- نتایج این مطالعه علمی به مراجع تصمیم‌ساز و تصمیم‌گیر جمهوری اسلامی ایران در تدوین و اتخاذ سیاست‌ها و راهبردها و الزامات تحقق آن کمک می‌نماید.

۳- بسترسازی برای تحقق اهداف کلان ملی در حوزه دفاعی – امنیتی بر اساس تدوین ارتباط بین اجـزاء در سـاختار معماری‌پایه فضای سایبر ملی

ضرورت تحقیق:

۱- برخورد منفعلانه در مواجهه با بحران‌های دفاعی – امنیتی

۲- فقدان یا ضعف در معماری کلان دفاعی- امنیتی در فضای سایبر ضمن تحمیل هزینه‌های زیاد، قدرت ملـی را در مواجهه بامخاطرات و چالشهای فضای سایبری کاهش می‌دهد .

سوال اصلی:

معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی– امنیتی چگونه است؟

سوالات فرعی:

۱. ویژگی‌های کلان حاکمیت در فضای سایبر کشور با رویکرد دفاعی- امنیتی کدامند؟
۲. مضامین راهبردی موثر بر معماری کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟
۳. اهداف و ماموریت‌های کلان مرتبط با فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟
۴. فرایندهای کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟
۵. ساختار کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟
۶. زیرساخت های فضای سایبر از منظر دفاعی-امنیتی چیست؟
۷. ارتباطات و تعاملات مولفه های معماری فضای سایبر از منظر دفاعی-امنیتی چیست؟

متغیرهای تحقیق:

متغیر مستقل: فضای سایبر جمهوری اسلامی با رویکرد دفاعی-امنیتی متغیر مستقل این تحقیق است.

متغیر وابسته: معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی-امنیتی متغیر وابسته این تحقیق است.

فرضیه‌های تحقیق:

با توجه به نوع تحقیق فرضیه‌ای برای این پژوهش متصور نیست.

۲. تعاریف و اصطلاحات:

معماری: معماری یعنی ارائه توصیفی فنی از یک سیستم که نشان‌دهنده ساختار اجزاء آن، ارتباط بین آنها، و اصـول و

قواعد حاکم بر طراحی و تکامل آنها در گذر زمان باشد(راهنورد و همکاران به نقل از آی تریپل ایی[1] ۱۳۸۶: ۲) این تعریف، تعریف پذیرفته شده در این مقاله است.

چارچوب معماری: راهنمایی برای تدوین معماری است. هر چارچوب معماری بسته به ماهیتی که دارد، متناسب سازمان خاصی است(معینی و همکاران ، ۱۳۹۴: ۲).

مدل شاو برای فضای سایبر: این مدل دارای سه سطح سیستمی, خدمات/محتوی و انسانی-اجتماعی می‌باشد که حاکمیت نیز بر هر سه این سطوح اعمال می‌شود (shaw, 2010: 1) که این مدل مبنا در این مقاله است.

امنیت: حفظ وجود و حیاط سالم و آرامش‌بخش انسان موکول به تامین همه نیازهای مادی و معنوی انسان است که در صورت عدم تامین و یا وجود تگنا یا نقص در تامین آن، حیات سالم و وجود انسان به چالش کشیده می‌شود و با تهدید روبرو می‌گردد و بلافاصله نیاز به امنیت و مفهوم آن در ارتباط با نیازهایی که با تنگنا روبرو شده در ذهن شکل می‌گیرد. « امنیت کامل و حقیقی قابل حصول نیست، بلکه انسان‌ها همواره تلاش می‌کنند تا تحت شرایط بالقوه معارض با امنیت، تا سر حد امکان امنیت افزایش پیدا کند.» (صنیعی، ۱۳۹۵: ۱۰)

امنیت ملی: رفع خطرات و ایجاد ایمنی برای حفظ ارزش‌های یک جامعه که در یک ملت و در قلمرو یک سرزمین زندگی می‌کنند و مرجع اصلی تامین آنها حکومت‌ها هستند. با توجه به اینکه ارزش‌های هر ملتی را می‌توان به بخش‌های مختلفی تقسیم کرد امنیت ملی نیز به شاخه‌های مختلف امنیت نظامی، اقتصادی، نرم‌افزاری و محیطی تقسیم می‌شود که باید باتوجه به اولویت‌بندی این ارزش‌ها به سیاست‌گذاری امنیت ملی پرداخت(صالح نیا، ۱۳۹۵: ۱). « باری بوزان» معتقد است که « امنیت ملی از لحاظ مفهومی، ضعیف و از نظر تعریف مبهم؛ اما از نظر سیاسی قدرتمند باقی مانده است» (همان به نقل از ماندل؛ ۱۳۷۹، ۴۰)

دفاع ملی: دفاع ملی در مقابل همه جنبه‌های تهدید، با استفاده از قدرت ملی و برای حفظ ، حمایت و دفاع از آرمان‌های ملی، اهداف ملی و منافع ملی شکل می‌گیرد. به عبارت دیگر دفاع ملی دفاعی همه جانبه است برای مقابله و مقاومت در برابر تهاجم و تجاوز (سخت و نرم) دشمن و تهدیدات امنیت ملّی در ابعاد مختلف آن و هر نیت و اقدام دشمن که باعث لطمه به ارزش‌های دینی و ملی گردد. به نحوی که بازدارنگی همه جانبه فراهم نماید و بازدارندگی نیز توان دفاعی را برای دفع تهدیدات تقویت کند. هسته مرکزی دفاع ملی را دفاع نظامی تشکیل می‌دهد، لکن دفاع ملی مفهومی فراتر از دفاع نظامی دارد و شامل همه مؤلفه‌های قدرت ملی می‌شود. .(دولتشاه ،۱۳۹۵ : ۸۶)

اقتدار دفاعی– امنیتی: آن دسته از اهداف ملی و ارزش‌های اسلامی هستند که برای بقاء و دوام یک ملت جنبه حیاتی دارند و ملت بقای خود را موکول به حفظ آنها می‌داند و در صورت به خطر افتادن این ارزش‌ها، ملت حاضر

[1] IEEE

به ایثار و فداکاری بوده و به جنگ خواهد پرداخت. (شریفی، ۱۳۹۵: ۳۵)

اهداف دفاعی– امنیتی: یکی از ابعاد اقتدار ملی است که شکل کارآمدی از مجموعه توانمندی‌های نظامی، انتظامی، اطلاعاتی، حفاظت و اطلاعات و بسیج مردمی یک کشور در چارچوب مشروع و مقبول در محیط امنیتی است. (دولتشاه ، ۱۳۹۵، ۳۱)

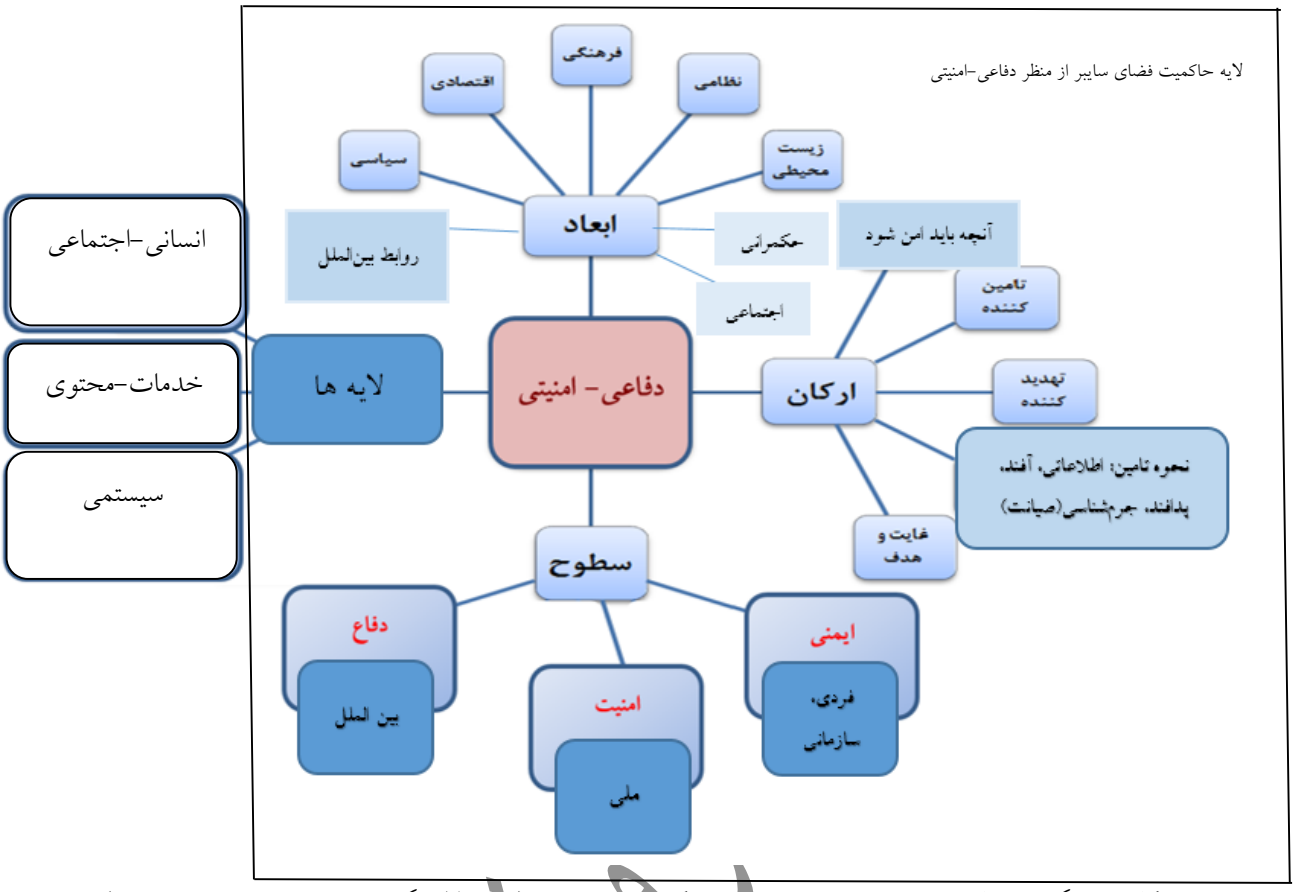
رویکرد دفاعی- امنیتی: تمرکز بر جنبه‌های دفاعی– امنیتی است و این تمرکز در سطح راهبردها و فرایندهای کلانی است که هماهنگی و هم‌افزائی لازم را برای بازیگران دفاعی–امنیتی در محیط درهمتنیده سایبری–فیزیکی فعلی برای تولید قدرت سایبری کشور در طراز جهانی فراهم کند(مطالعه گروهی داعا،۱۴۰۰ :۱۶).

۳. پیشینه:

در رساله با عنوان ارائه الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی(هلیلی، ۱۳۹۸ : ۱۹) چگونگی الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی سئوال اصلی است. در این رساله، برای طراحی الگوی راهبردی ارتقاء قدرت سایبری که مقوله‌ای در حوزه سیاستگذاری کلان و راهبردی است از رویکرد نظری- مفهومی استفاده شده است. در این رویکرد، تمرکز بر عمق موضوع و مطالعه عناصر و روابط بین آنهاست و فرایندها و رویه‌ها، کمتر مورد تاکید هستند. برای این کار، با توجه به پیچیدگی و گستردگی موضوع، پس از تعیین مهمترین متغیرها و عوامل موثر در بخش مبانی نظری پایه و تحلیل محیطی، از طریق مطالعات اکتشافی، مهمترین اجزاء قدرت سایبری و روابط بین آنها استخراج گردید. این فرایند با در نظر گرفتن مبانی ارزشی و نظم بخشیدن به واقعیتهای موجود صورت گرفت؛ تا یک الگوی جامع و پویا بدست آید. نصرت‌آبادی نیز در رساله ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ا(نصرت آبادی، ۱۳۹۸) سعی در پاسخگویی به این سئوال دارد که الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.اکدام است؟ در این رساله قدرت سایبری در سه بعد آفند، پدافند و تاب¬آوری سایبری برای ارزیابی مورد توجه قرار گرفته است.

۴. ویژگیهای کلان حاکمیت در فضای سایبر با رویکرد دفاعی-امنیتی:

با مقایسه مدل شاو و شکل ذیل به خوبی می‌توان دریافت که شکل ذیل عملاً بسط لایه حاکمیت در مدل شاو است و از زاویه دیگر ویژگی‌های معماری کلان فضای سایبر را با رویکرد دفاعی–امنیتی نشان داده است(**منبع:مطالعه گروهی داامنیت – داعا، ۱۴۰۰: ۱۰۲).**



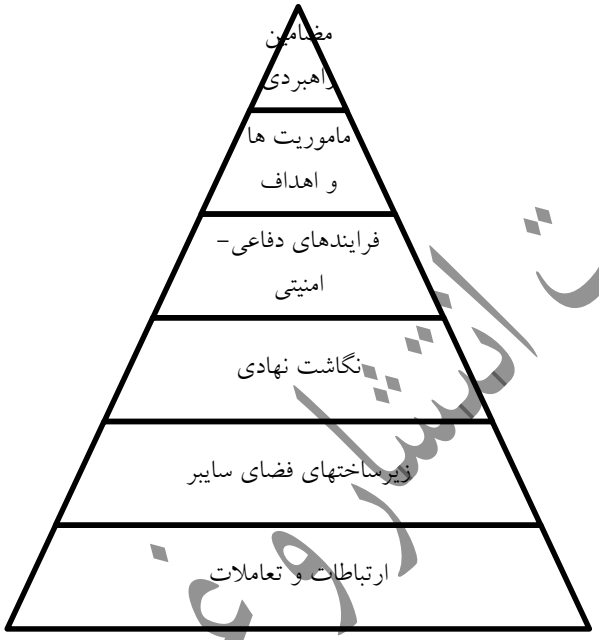
شکل ۱– ویژگی‌های کلان حاکمیت در فضای سایبر با رویکرد دفاعی– امنیتی(منبع:مطالعه گروهی داامنیت – داعا، ۱۴۰۰: ۱۰۲)

در ارکان شکل مذکور غایت و هدف رویکرد دفاعی–امنیتی برای فضای سایبر ارائه شده است. در ارکان شکل مذکور چهار فرایند اطلاعاتی، آفند، پدافند و صیانت یا جرم‌شناسی سایبری مشخص شده‌اند. « پدافند » شامل اقدامات مربوط به امن سازی، تشخیص حملات، مقابله با حملات و بازیابی از حمله است(Andress، et.al ، ۲۰۱۴: ۵۴). « آفند » شامل اقداماتی از قبیل شناسایی دارائی‌های دشمن، شناسایی آسیب‌پذیری‌های دارائیهای مذکور، ایجاد قابلیت بهره‌برداری و سناریونویسی و نهایتاً طراحی و در صورت نیاز اجرای حمله است. اطلاعاتی نیز فرایندی مشابه آفند دارد جز اینکه هدف آن سرقت اطلاعات است و نه تغییر و تخریب. در جرم‌شناسی نیز آماده‌سازی روش و ابزار، جمع‌آوری شواهد، تحلیل شواهد و تهیه گزارش برای دادگاه است(Andress، et.al ، ۲۰۱۴ : ۲۴۱). با این توصیف و با توجه به شکل ۱، ویژگی‌های فضای سایبر از منظر دفاعی و امنیتی در چهار سطح و چهار حوزه برای مقابله با سه سطح تهدید توسط سازمان‌های دفاعی–امنیتی به منظور حفاظت از دارائیهای سیاسی، اقتصادی، فرهنگی، اجتماعی و ... قابل تعریف است. سطح سیستمی یا زیرساختی از منظر جرم‌شناسی، اطلاعاتی، پدافند و آفند، سطح کاربرد/محتوی از منظر جرم‌شناسی(صیانتی)، اطلاعاتی، پدافند و آفند و سطح انسانی–اجتماعی از منظر جرم-شناسی(صیانتی)، اطلاعاتی، پدافند و آفند و سطح حاکمیتی از منظر جرم‌شناسی(صیانتی)، اطلاعاتی، پدافند و آفند. و هر یک از این سطوح و حوزه‌ها با عنایت به سه سطح تهدید فردی و درون سازمانی، ملی و فراملی به منظور حصول ایمنی، امنیت و دفاع سایبری نقش‌هایی را برای دستگاه‌های تامین کننده دفاعی–امنیتی با هدف تامین اهداف

مرتبط با ابعاد(دارائیهای) سایبریِ سیاسی، اقتصادی، اجتماعی، فرهنگی و ... تعیین می‌کند(**منبع:مطالعه گروهی داامنیت - داعا، ۱۴۰۰: ۱۰۲)**.

۵. چارچوب و مضامین راهبردی در معماری کلان:

ما در این مقاله چارچوب معماری کلان فضای سایبر با رویکرد دفاعی-امنیتی مطابق شکل۲ را مبنای کار قرار دادیم (منبع:مطالعه گروهی داامنیت - داعا، ۱۴۰۰: ۱۱۷).



شکل۲- چارچوب معماری کلان فضای سایبر با رویکرد دفاعی-امنیتی(منبع:مطالعه گروهی داامنیت - داعا، ۱۴۰۰: ۱۱۷)

و دو مضمون راهبردی:

۱- تقویت حاکمیت با تمرکز بر استقلال از طریق صیانت از مشروعیت(در سطح ملی و بین الملل)، کارآمدی(مقابله با تهدیدات در سطح فردی، سازمانی، ملی و بین‌المللی) و نفوذ و
۲- بازتعریف حاکمیت با تمرکز بر استقلال" نقش مردم ، جغرافیای سرزمینی ، منابع ملی و نظام حکومتی "

را به عنوان مضامین راهبردی در این مقاله مورد استفاده قرار خواهیم داد.**(منبع:مطالعه گروهی داامنیت - داعا، ۱۴۰۰: ۱۳۳)**

۶. روش‌شناسی تحقیق

با توجه به موضوع وهدف پژوهش، نوع پژوهش کاربردی- توسعه‌ای[1]است. این پژوهش ازآنجا که بنا به نیاز سازمان‌ها و نهادهای دفاعی امنیتی انجام شده است، پژوهشی کاربردی است و از طرفی چون از منظر امنیت ملی جمهوری اسلامی ایران، باعث بهبود روش‌ها وساختارهای دفاعی-امنیتی با توجه به تحولات مرتبط با فضای سایبر

[1]Applied – Development Research

می‌شود، به ارتقاء امنیت ملی کمک نموده و جزء تحقیق‌های توسعه‌ای تلقی می‌شود.

روش تحقیق در این پژوهش هم برای پاسخ به سئوالات تحقیق و هم برای ارزیابی نتایج، کیفی است به اینصورت که ابتدا با مراجعه به مقالات و اسناد علمی سعی در پاسخگویی به سئوالات تحقیق شد سپس با استفاده از روش گروه کانونی و با استفاده از معیارهای روایی و پویایی کیفی از جمله باورپذیری، انتقال‌پذیری، قابلیت اعتماد و تائید-پذیری نتایج مورد ارزیابی و تائید قرار گرفته است. بدین منظور بر اساس روش کیفی گروه کانونی و با استفاده از دیدگاه صاحب‌نظران چارچوب معماری کلان فضای سایبر از منظر دفاعی امنیتی انتخاب و در ادامه با روش کیفی گروه کانونی فرایند و نگاشت نهادی مطابق با چارچوب معماری انتخاب شده بدست آمد. در مرحله بعد با روش کیفی گروه کانونی و بر اساس شاخص‌های باورپذیری، انتقال‌پذیری، قابلیت اعتماد و تائیدپذیری معماری حاصل مورد ارزیابی و تائید قرار گرفت.

با توجه به موضوع پژوهش، مقتضیات مسئله ایجاب نمود که جامعه آماری کسانی باشند که در حوزه مسایل اجتماعی، فضای سایبر، رسانه‌ها و شبکه‌های اجتماعی دارای شناخت وآگاهی باشند لذا جمعیت آماری این تحقیق بر اساس مشاوره با اساتید دانشگاهی و خبرگان این حوزه عبارتند از:

– اساتید و کارشناسان درحوزه‌های فضای سایبر، ارتباطات، رسانه، شبکه‌های اجتماعی مجازی که در قالب دو گروه کانونی ۶ تا۹ نفره با زمینه‌های تخصصی متفاوت و البته مرتبط با موضوع تحقیق سازماندهی شده‌اند.

در این پژوهش از دو شیوه نمونه‌گیری غیر احتمالی یعنی نمونه‌گیری با استفاده از روش نمونه‌گیری هدفمند / معیار محور (انتخاب تمام موردها با انتخاب معیار خاص) استفاده شد. در این روش نمونه گیری، هدف آن است که از طریق افراد انتخاب شده درک عمیقی از موضوع مورد مطالعه حاصل شود و اعضای نمونه کسانی هستند که اطلاعات غنی و مناسبی راجع به موضوع تحقیق دارند. حجم نمونه با توجه به اینکه جمعیت گروه‌های کانونی کمتر از ۲۰ نفر بوده است به صورت تمام شمار می‌باشد.

با عنایت به چارچوب معماری پیشنهادی در شکل(۲) و مضامین راهبردی مرتبط، به منظور ارائه معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی–امنیتی ابتدا با استفاده از روش گروه کانونی اقدام به استخراج ماموریت‌ها و اهداف سیاسی–امنیتی با توجه به موضوع تحقیق شد که در ادامه با همین روش استخراج فرایند دفاعی–امنیتی انجام شد و در انتها با توجه به ماموریت‌ها و اهداف سازمان‌های دفاعی–امنیتی و فرایند دفاعی–امنیتی اقدام به نگاشت نهادی ماموریت‌های هر سازمان به فرایند دفاعی و امنیتی و از این رهگذر معماری کلان فضای سایبر ج.ا.ا ارائه شد. نتایج تحقیق نیز با استفاده از روش گروه کانونی صحه‌گذاری شد.

در پژوهش‌های کیفی، معیارهای مختلفی معادل با روایی و پایایی در نظر گرفته شده است. لینکولن و گوبا چهار معیار برای ارزیابی یک پژوهش کیفی پیشنهاد داده‌اند که در جدول۱ بطور خلاصه توضیح داد شده است (محمدپور، ۱۳۸۷: ۸۱).

جدول۱– معیارهای تحقیق کیفی(محمدپور، ۱۳۸۷:۸۱)

معیار	توصیف

معیار	توصیف
باور پذیری[1]	معادل روایی داده‌های ورودی تحقیق و کدهای توصیفی و تفسیری اختصاص داده شده است. بنابراین یافته‌های پژوهش و کدهای اختصاص داده شده به نظرات مصاحبه شوندگان به آنها ارایه می‌شود تا مورد تایید آنها قرار گیرد.
انتقال پذیری [2]	نشان می‌دهد اگر تحقیق در محیط متفاوت و برای جامعه آماری متفاوت انجام شود چه نتایجی حاصل می‌شود. برای این منظور باید از مصاحبه شوندگان متنوع که در گروه‌ها (سازمان‌های) مختلف هستند استفاده شود.
قابلیت اعتماد [3]	میزان توانایی ابزار انسانی برای کسب نتایج سازگار و منطقی را نشان می‌دهد. روش‌ها و تصمیم‌های اتخاذ شده با هدف بازبینی و موشکافی پژوهش در اختیار دیگر پژوهشگران قرار می‌گیرد.
تایید پذیری [4]	محقق باید نشان دهد که یافته‌های او عملا و واقعا مبتنی بر داده‌ها هستند. بنابراین در این معیار گزیده مصاحبه‌ها و توضیح روند تحلیل داده‌ها برای تایید عملی و واقعی بودن ارایه می‌شود.

در این تحقیق ما برای صحه‌گذاری نتایج تحقیق از روش گروه کانونی استفاده کردیم. در این روش از ۲ گروه کانونی ۶ تا۹ نفره با زمینه‌های تخصصی متنوع استفاده شده است.

طبق تعریف مرسوم، پژوهش گروه کانونی شیوه‌ای برای جمع آوری داده‌های کیفی است که افراد را در یک بحث گروهی غیررسمی (یا چندین بحث) پیرامون موضوعی خاص یا مجموعه‌ای از موضوعات وارد می‌کند معمولاً پژوهشگران علوم اجتماعی بطور کلی و همچنین محققان کیفی به طور ویژه، برای جمع آوری همزمان داده‌ها از تعدادی از افراد، به تشکیل گروه‌های کانونی مبادرت می‌ورزند. گروه‌های کانونی برای بسیاری از افراد شرکت کننده در پژوهش کمتر تهدیدکننده تلقی می‌شوند زیرا محیط مناسبی را برای بحث درباره ادراکها، ایده‌ها، عقاید و افکار آنان فراهم می‌آورند تعامل بین اعضای گروه، ویژگی کلیدی و مهم این شیوه تحقیقی است که براساس آن گروه‌های کانونی از مصاحبه گروهی که تعاملی بین مصاحبه گر و مصاحبه شونده است، متمایز می‌شوند. در این موقعیت گروهی، افراد با پویایی و انرژی به دیدگاه‌های دیگر واکنش نشان می‌دهند، به طوری که طرح تنها یک پیشنهاد یا موضوع می‌تواند زنجیره‌ای از پاسخها و واکنشها را از سوی حاضران ایجاد کند. این نوع تعامل با عنوان تأثیر «هم نیروزادی» توصیف می‌شود که بر همین اساس، برخی پژوهشگران معتقدند در گروه‌های کانونی اطلاعات به نسبت بیشتری در مقایسه با شیوه‌های پژوهشی دیگر به دست می‌آید. گروه کانونی، بحثی گروهی است که پیرامون موضوع یا موضوع هایی خاص تمرکز می‌یابد و به این ترتیب، واژه کانونی به این نکته اشاره می‌کند. (حسینی، ۱۳۹۴: ۱۴-۱۵) . در این تحقیق ما از قابلیت‌های گروه کانونی برای صحه‌گذاری بر یافته‌های تحقیق استفاده کردیم

---

[1] Credibility
[2] Transferability
[3] Dependability
[4] Confirmability

۷. تجزیه و تحلیل یافته‌ها

ما در این مقاله از چارچوب معماری شکل ۲ و نیز دو مضمون راهبردی که در بخش ۵ این مقاله به آن اشاره شده برای استخراج معماری کلان استفاده می‌کنیم.

ماموریت‌ها و اهداف کلان دفاعی-امنیتی در فضای سایبر:

در این قسمت با روش گروه کانونی اقدام به استخراج ماموریت‌ها و اهداف کلان دفاعی-امنیتی کردیم که در جدول(۲) ارائه شده است. ماموریت‌ها و اهداف کلان متعدد مورد بحث قرار گرفت و برخی انتخاب شدند. کنار آنهائیکه انتخاب شده‌اند یک عدد است که ارتباط هدف مورد نظر را با مضمون راهبردی هم‌شماره که در بخش ۵ مقاله به آن اشاره شده است مشخص می‌کند عبارت‌های آفند و پدافند و غیره نیز ارتباط هدف با فرایندهایی را که در مرحله بعد نحوه استخراج آنها بیان شده است مشخص می‌کند.

جدول(۲)- ماموریت و اهداف کلان دفاعی-امنیتی فضای سایبر

ردیف	ماموریت‌ها و اهداف کلان دفاعی امنیتی فضای سایبر	شماره مضمون راهبردی مرتبط	فرایند دفاعی-امنیتی مرتبط
۱	دستیابی به توان بازدارندگی در مقابل انواع تهدیدات و حملات و سایبری	۱	آفندی، اطلاعاتی، صیانتی
۲	دستیابی به بالاترین سطح توان و قابلیت‌های دفاعی (افند و پدافند) در فضای سایبر	۱	آفند و پدافند
۳	اشراف و تسلط پایدار و جامع بر فضای مجازی و سایبری کشور	۱	اطلاعاتی
۴	دستیابی به توان نرم(شناخت) در فضای مجازی در مقابله با تهدیدات بیگانگان	۱	پدافند
۵	دستیابی به بالاترین سطح امنیت و حفاظت برای صیانت موثر از سرمایه‌ها و منابع سایبری کشور	۲	پدافند
۶	دستیابی به بالاترین سطح امنیت و حفاظت برای صیانت موثر از زیرساخت‌های حیاتی و حساس و مهم کشور	۲	پدافند
۷	برخورداری از قدرت پیش بینی تهدیدات و فرصتها جهت جلوگیری از غافلگیری و غافلگیر کردن دشمن	۱	اطلاعاتی
۸	تاب آوری ملی در ابعاد اجتماعی، زیرساختی و اطلاعاتی	۱	پدافند
۹	استقرار نظم و امنیت و تأمین آسایش عمومی و فردی	۱	صیانتی
۱۰	ساماندهی و تامین یکپارچه نیازمندیهای کشور با تاکید استفاده حداکثری از توان داخلی	۱	توانمند سازی

افراز فرایندهای اصلی دفاعی-امنیتی فضای سایبری:

در این بخش برای استخراج فرایند دفاعی امنیتی و ارتباط آن با فضای سایبر از روش گروه کانونی استفاده شد. در ادامه با استفاده از چارچوب معماری شکل(۲) و افراز فضای سایبر و با عنایت به سه سطح فردی-سازمانی، ملی و منطقه‌ای-بین‌المللی و بر اساس دسته‌بندی انجام شده برای مضامین راهبردی، فرایند دفاعی-امنیتی را می‌توان در پنج حوزه پدافند و آفند و اطلاعات و صیانت امنیتی و توانمندسازی در فضای سایبر با عنایت به نگاه کلان به معماری با روش گروه کانونی مورد بررسی قرار داد که نتایج در جداول(۳)و(۴)ارائه شده است.

فرایند پدافند:

همانطور که در جدول ۳ مشاهد می‌شود در حوزه پدافند فرایندی شامل چهار مرحله امن‌سازی و بازدارندگی، تشخیص حملات، مقابله با حملات و بازیابی از حمله(راه‌اندازی مجدد سیستم) است که باید در سه سطح انسانی- اجتماعی شامل موضوعات اقتصادی، سیاسی، فرهنگی، اجتماعی و غیره، سطح خدمات، محتوا و سطح سیستمی فضای سایبر به منظور تامین ایمنی، امنیت و دفاع کشور مورد توجه قرار گیرد از آنجائیکه در این تحقیق هدف ما ارائه معماری کلان است به اقدامات ذیل لایه‌های فضای سایبر اشاره نشده است. نکته قابل توجه در این خصوص این است که باید در کل فرایند پدافند اقدامات مربوط به ریسک‌های آینده تحت تاثیر روندهای فناوری مورد ملاحظه قرار گیرد.

جدول۳- جدول فرایند پدافند

فضای سایبر	مراحل فرایند پدافند	سطوح تهدید و آسیب‌پذیری
لایه های فضای سایبر شامل سیستمی، خدمت- محتوی و انسانی-اجتماعی(مدل مبنا در این مقاله)	امن‌سازی و بازدارندگی	هر سه سطح فردی- سازمانی، ملی، بین‌الملل و با نگاه به آینده
	تشخیص حملات	
	مقابله با حملات	
	بازیابی از حملات	

فرایند آفند و فرایند اطلاعاتی:

همانطور که در جدول ۴ دیده می‌شود فرایند آفند شامل چهار مرحله شناسایی سرمایه‌ها و دارائیهای حیاتی دشمن و آسیب‌پذیریهای این دارائیها و سپس ایجاد ابزارهای بهره‌برداری از این آسیب‌پذیریها و طراحی حمله و نهایتاً اجرای حمله است. این حملات می‌تواند در هریک از سه سطح انسانی-اجتماعی، خدمات/محتوا و سیستمی فضای سایبر بر روی افراد، سازمان‌های دولتی، مجموعه‌ای از زیرساخت‌های ملی و حتی در سطح دارائیهای بین‌المللی دشمن صورت بگیرد. بدیهی است که این فرایند باید با توجه به روندهای فناوری و آسیب‌پذیریهایی که در اثر آنها برای دشمن انجام می‌شود نیز مورد توجه قرار گیرد. با توجه به اینکه موضوع تحقیق معماری کلان است وارد مضاین ذیل لایه های فضای سایبر نشده‌ایم. در خصوص فرایند اطلاعاتی همان فرایند آفند است با این تفاوت که به جای مرحله اجرای حمله مرحله بهره‌برداری است زیرا در آفند اقدام به دسترسی برای تخریب می‌شود و در فرایند اطلاعاتی دسترسی با هدف سرقت اطلاعات و یا جعل صورت می‌گیرد که بصورت خلاصه تحت عنوان مرحله بهره‌برداری از آن یاد می‌شود.

جدول۴- جدول فرایند آفند و اطلاعاتی

فضای سایبر	مراحل آفند	سطوح حمله به دشمن
لایه های فضای سایبر شامل سیستمی، خدمت- محتوی و	شناسایی دارائیهای حیاتی دشمن	حملات به دشمن در هر سه سطح فردی- سازمانی، ملی، بین‌الملل و با نگاه به آینده
	استخراج آسیب‌پذیریهای دارائیهای حیاتی دشمن	

انسانی-اجتماعی	ایجاد قابلیت بهره‌برداری از آسیب‌پذیری و طراحی حمله	
	اجرای حمله	

فرایند صیانتی:

فرایند جرم‌شناسی(صیانت) نیز که فرایند محوری صیانت از نظم و امنیت عمومی است نیز با همین رویکردی که در خصوص سه فرایند دیگر استحصال شده است قابل حصول است این فرایند نیز در سه سطح فردی-سازمانی، ملی و بین‌المللی قابل تعریف است در چهار مرحله تامین ابزارها، جمع‌آوری شواهد، شناسایی عامل و چگونگی جرم و نهایتا تهیه گزارش قابل قبول برای دادگاه است که در هر سه سطح سیستمی، خدمت/محتوا و انسانی-اجتماعی فضای سایبر قابل اعمال است.

فرایند توانمند سازی:

این فرایند با عنایت به مطالعات تطبیقی شامل حوزه‌های مهم توسعه علم و فناوری، صنعت و نوآوری، قانون‌گذاری و حوزه قضایی و حوزه دیپلماسی است. توسعه سامانه‌ها و زیرساخت‌های بومی امنیت ساز در مدیریت فضای سایبری کشور دارای اهمیت ویژه بوده که نباید به خارج وابسته باشد؛ از طرفی تقویت نهاد قضائی و به تبع آن قوانین و مقررات سایبری دارای اهمیت ویژه ای است که در معماری نوین قضایی سایبری باید مورد توجه قرار گیرد.

ساختار کلان فضای سایبر ج.ا.ا با رویکرد دفاعی-امنیتی:

نتایج مباحثات در گروه کانونی نشان داد که ساختار کلان فضای سایبر با رویکرد دفاعی-امنیتی شامل دو بخش اصلی است که عبارتند از:

- نگاشت نهادی و ارتباطات نهادهایی است که فرایندهای دفاعی-امنیتی را اجرا می‌کنند.
- قلمروهایی که این نهادها فرایندهای مذکور را در آن اجرا می‌نمایند.

لایه‌های فضای سایبر	فرایندهای دفاعی-امنیتی	سازمان مجری	سازمان همکار	سازمان هماهنگ کننده-سیاست‌گذار	سطوح دفاعی-امنیتی شامل فردی-سازمانی، ملی، بین-المللی
قلمروهای دفاعی-امنیتی ج.ا.ا در فضای سایبر(قلمرو نظامی، قلمرو امنیتی، قلمرو توسعه و مرز کل این قلمروها با تهدیدات بیرونی)					

شکل۳- ساختار کلان فضای سایبر با رویکرد دفاعی-امنیتی

نگاشت نهادی:

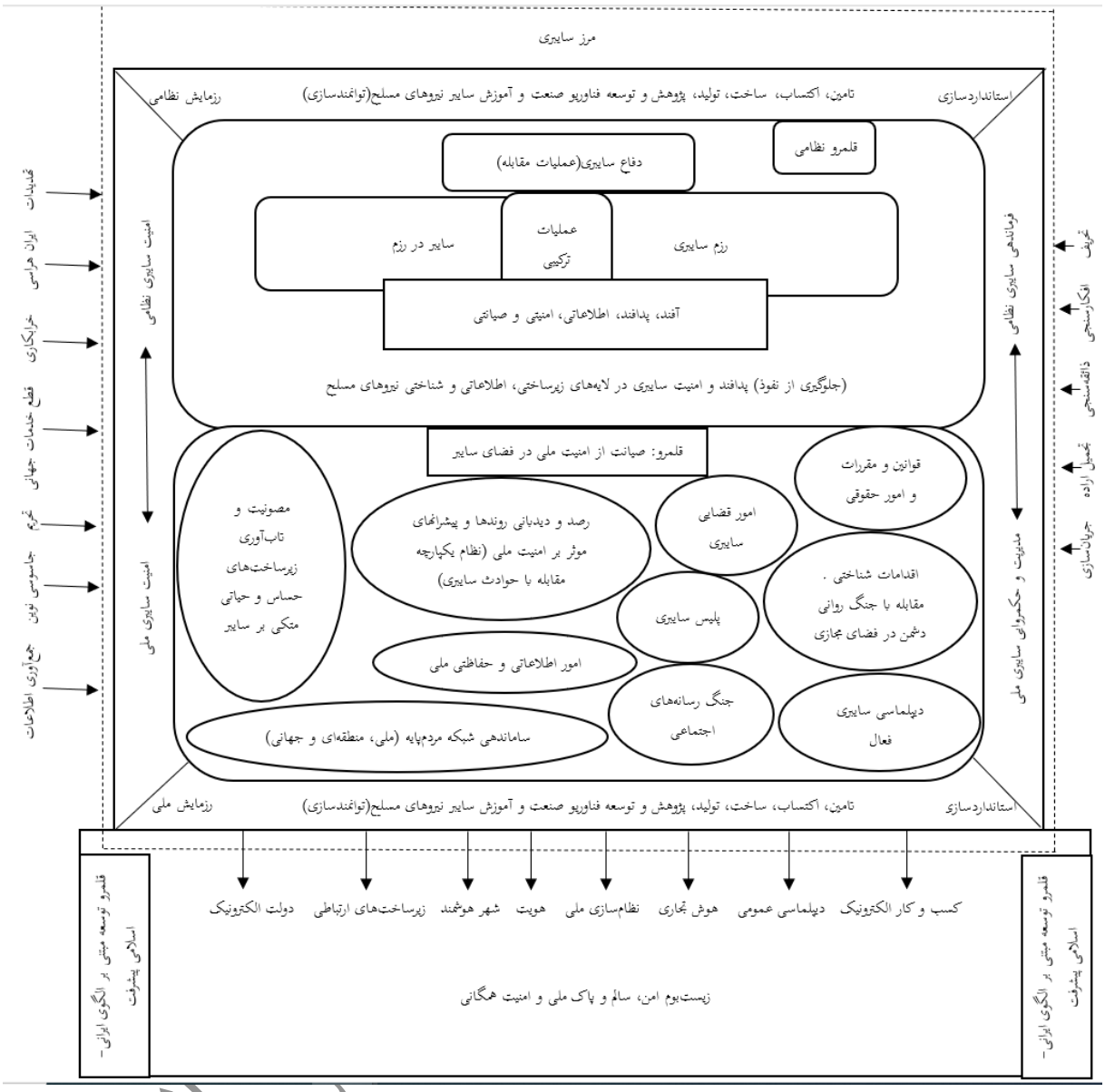
ساختار پیشنهادی با توجه به فرایند استخراج شده برای پدافند و آفند، اطلاعاتی، صیانتی و توانمندسازی بانگاه ایمنی در سطح داخل سازمان و با نگاه امنیت در سطح ملی و با نگاه دفاع در سطح فراملی معنا پیدا می‌کند. با توجه به وظائف قانونی نهادهای دفاعی-امنیتی سه نقش اساسی برای آنها متصور است نقش مجری، نقش همکار و نقش هماهنگ‌کننده-سیاست‌گذار. ساختار پیشنهادی در سطح سازمان‌های دولتی و خصوصی و عموم مردم با مفهوم ایمنی، در سطح ملی با مفهوم امنیت و در سطح فراملی با مفهوم دفاع تعریف شده است و همانطور که بطور ضمنی بیان شده است در سه سطح تهدید فردی-داخل سازمانی، ملی و فراملی تعریف شده اگر چه از نظر فرایند در هر سه سطح مشابه و از نظر ابعاد متفاوت هستند.

ارتباطات نهادی:

سازمان‌های دفاعی و امنیتی و غیر آنها مسئول تامین ایمنی خود هستند. سازمان‌های مسئول امنیت ملی و امنیت عمومی مسئول تامین امنیت سایبری در سطح ملی هستند که ذیل شورای عالی امنیت ملی و یا شورای عالی فضای مجازی متناسب با شکل و سطح حادثه با هم هماهنگ می‌شوند و در صورت نیاز به هماهنگی با دستگاه‌های دیگر نیز در همین چارچوب هماهنگ می‌شوند. سازمان‌های نظامی با هماهنگی ستاد کل نیروهای مسلح مسئول تامین دفاع سایبری هستند و در صورت نیاز به هماهنگی با دستگاهای دیگر در چارچوب شورای عالی امنیت ملی با هم هماهنگ می‌شود.

قلمرو دفاعی-امنیتی ج.ا.ا در فضای سایبر:

قلمروهای مختلف مرتبط با حوزه‌های دفاعی-امنیتی که فرایندهای دفاعی-امنیتی در آنها اجرا می‌شود شکل ۴ مشخص شده است که عبارتند از قلمرو نظامی، قلمرو امنیتی، قلمرو توسعه و مرز کل این قلمروها با تهدیدات بیرونی.



شکل۴- نمایی از قلمرو دفاعی-امنیتی ج.ا.ا در فضای مجازی

زیرساخت های فضای سایبر از منظر دفاعی-امنیتی:

با توجه به مباحثات گروه کانونی زیرساخت‌های فضای سایبر شامل دو بخش هستند که عبارتند از:

- زیرساخت‌های مربوط به فرایندهای تهاجمی مثل آفندی و اطلاعاتی
- زیرساخت‌های مربوط به فرایندهای دفاعی- مثل پدافندی و صیانتی

که در ادامه توضیح داده خواهد شد.

زیرساخت فرایندهای پدافند و صیانتی:

در این مقاله زیرساخت فضای سایبر از منظر فرایندهای پدافند و صیانتی با توجه به الزامات قانونی شبکه ملی اطلاعات است. اما آنچه در این کار گروهی مورد تاکید است قابلیت‌هایی است که شبکه ملی اطلاعات از منظر

دفاعی-امنیتی باید داشته باشد. وقتی از زاویه این زیرساخت به شکل ۴ نگاه کنیم متوجه می‌شویم که شبکه ملی اطلاعات باید دو نیازمندی اساسی را تامین نماید که عبارتند از:

- قابلیت محافظت از مرز سایبری در مقابل تهدیدات مثل قطع خدمات جهانی، تحریم، جمع‌آوری اطلاعات، خرابکاری و ...
- قابلیت ایجاد زیست‌بوم امن، سالم، پاک ملی و امنیت همگانی برای ایجاد دولت الکترونیک، کسب وکار الکترونیک، شهر هوشمند، هوش تجاری و ...

زیرساخت فرایندهای آفند و اطلاعاتی:

این زیرساخت بیشتر تمرکز بر شبکه‌هایی دارد که توسط آنها امکان دسترسی به دارائیهای حیاتی دشمن وجود دارد.

ارتباطات و تعاملات مولفه های معماری فضای سایبر از منظر دفاعی-امنیتی:

شکل ۵ نحوه ارتباطات و تعاملات مولفه‌های مختلف معماری را که در چارچوب معماری شکل ۲ مشخص شده و در بخش‌های قبل بدست آمده را نشان می‌دهد.

ردیف	مضمون راهبردی مرتبط	ماموریت‌ها و اهداف کلان دفاعی امنیتی فضای سایبر	فرایند دفاعی-امنیتی مرتبط	نگاشت نهادی	سطوح دفاعی-امنیتی	فضای سایبر
۱	۱	دستیابی به توان بازدارندگی در مقابل انواع تهدیدات و حملات و سایبری	آفند، اطلاعاتی، صیانتی	مجری، همکار، سیاتگذار-هماهنگ کننده	فردی-سازمانی، ملی، بین-المللی	لایه های فضای سایبر
۲	۱	دستیابی به بالاترین سطح توان و قابلیت‌های دفاعی (افند و پدافند) در فضای سایبر	آفند و پدافند			
۳	۱	اشراف و تسلط پایدار و جامع بر فضای مجازی و سایبری کشور	اطلاعاتی			
۴	۱	دستیابی به توان نرم(شناخت) در فضای مجازی در مقابله با تهدیدات بیگانگان	پدافند			
۵	۲	دستیابی به بالاترین سطح امنیت و حفاظت برای صیانت موثر از سرمایه‌ها و منابع سایبری کشور	پدافند			
۶	۲	دستیابی به بالاترین سطح امنیت و حفاظت برای صیانت موثر از زیرساخت‌های حیاتی و حساس و مهم کشور	پدافند			
۷	۱	برخورداری از قدرت پیش بینی تهدیدات و فرصتها جهت جلوگیری از غافلگیری و غافلگیر کردن دشمن	اطلاعاتی			

۸	۱	تاب آوری ملی در ابعاد اجتماعی، زیرساختی و اطلاعاتی	پدافند			
۹	۱	استقرار نظم و امنیت و تأمین آسایش عمومی و فردی	صیانتی			
۱۰	۱	ساماندهی و تامین یکپارچه نیازمندیهای کشور با تاکید استفاده حداکثری از توان داخلی	توانمند سازی			
قلمروهای دفاعی–امنیتی ج.ا.ا در فضای سایبر(قلمرو نظامی، قلمرو امنیتی، قلمرو توسعه و مرز کل این قلمروها با تهدیدات بیرونی)						
زیرساخت‌های فضای سایبر از منظر دفاعی–امنیتی						

شکل۵- ارتباطات و تعاملات مولفه‌های معماری فضای سایبر از منظر دفاعی–امنیتی

معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی–امنیتی:

مولفه‌های شکل۵ که در بخش‌های مختلف این مقاله آمده است و نحوه تعامل آنها عملاً معماری کلان فضای سایبر ج.ا.ا را با رویکرد دفاعی—امنیتی را تبیین می‌کنند یعنی ارتباط بین مضامین راهبردی (مستخرج از فرامین مقام معظم رهبری(مدظله)، اسناد بالادستی، مطالعات تطبیقی و روندهای فناوری) با اهداف و ماموریت‌های کلان دفاعی–امنیتی فضای سایبر و نیز فرایندهای دفاعی– امنیتی را برقرار می‌نماید و ارتباط آنها با نگاشت نهادی و لایه‌های فضای سایبر مشخص شده است علاوه بر این، این ارتباط با قلمروهای دفاعی–امنیتی و نیز زیرساخت‌های مورد نیاز این حوزه تبیین گردیده است. وقتی به این معماری از زاویه فرایندها و زیرفرایندهای آن نگاه کنیم متوجه می‌شویم که این معماری در حقیقت ارائه دهنده پنج نظام و زیر نظام‌های مرتبط با آنها در فضای سایبر ج.ا.ا با رویکرد دفاعی–امنیتی نیز هست که منظومه کلان دفاعی–امنیتی ج.ا.ا در فضای سایبر را تشکیل می‌دهند. این نظام‌ها عبارتند از

نظام پدافند سایبری شامل:

زیرنظام امن‌سازی و بازدارندگی

زیرنظام تشخیص حملات

زیرنظام مقابله با حملات

زیر نظام بازیابی از حملات

نظام آفند سایبری شامل:

زیر نظام شناسایی دارائیهای حیاتی دشمن

زیرنظام استخراج آسیب‌پذیریهای دارائیهای حیاتی دشمن

زیرنظام ایجاد قابلیت بهره‌برداری از آسیب‌پذیری و طراحی سناریوی حمله

زیرنظام اجرای حمله

نظام اطلاعات سایبری شامل:

زیر نظام شناسایی دارائیهای حیاتی دشمن

زیرنظام استخراج آسیب‌پذیریهای دارائیهای حیاتی دشمن

زیرنظام ایجاد قابلیت بهره‌برداری از آسیب‌پذیری

زیرنظام بهره برداری اطلاعاتی و اشراف ملی در فضای سایبری

نظام صیانت سایبری شامل:

زیر نظام تهیه ابزار

زیرنظام جمع‌آوری شواهد

زیر نظام تحلیل اطلاعات و شناسایی چگونگی وقوع جرم و عامل جرم

زیر نظام تهیه گزارش برای قاضی

نظام توانمند سازی سایبری:

زیرنظام علمی و فناوری و آموزش

زیر نظام صنعت و نوآوری سامانه ها و تجهیزات بومی

زیر نظام قانون‌گذاری

زیرنظام قضایی

زیرنظام برنامه ریزی راهبردی(دکترین سیاست گذاری، راهبرد و برنامه ریزی)

زیر نظام ساختار و سازمان(فرماندهی، نگاشت نهادی و تنظیم روابط و ارتباطات) و مدیریت منابع

زیرنظام دیپلماسی و قوانین بین الملل

زیر نظام رسانه‌های اجتماعی و مقابله با جنگ رسانه ای و شناختی

ارزیابی معماری ارائه شده:

معماری ارائه شده با روش گروه کانونی و بر اساس معیارهای جدول ۱ یعنی باورپذیری، انتقال‌پذیری، قابلیت اعتماد و تائیدپذیری مورد ارزیابی قرار گرفت که نتایج در ذیل ارائه شده است.

باورپذیری:

کلیات معماری کلان به تایید اعضای گروه کانونی رسید و تطبیق نتایج با دیدگاه‌های آنها مورد تائید قرار گرفت.

انتقال پذیری:

به این منظورمعماری ارائه شده به چند گروه ارائه شد که پس اصلاحات مورد نظر مورد تائید ایشان قرار گرفت

قابلیت اعتماد:

به این منظورمعماری ارائه شده به گروه‌های مذکور ارائه شد که مورد تائید ایشان قرار گرفت.

تائیدپذیری:

به این منظورمعماری ارائه شده به گروه‌های مختلف ارائه شد که مورد تائید ایشان قرار گرفت

با عنایت به نتایج ارزیابی مشخص شد که معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی-امنیتی بر اساس قواعد علمی مورد تائید است.

۸. نتیجه‌گیری

در این بخش اقدام به پاسخ به سوالات فرعی می‌کنیم:

۱. ویژگی‌های کلان حاکمیت در فضای سایبر کشور با رویکرد دفاعی- امنیتی کدامند؟ پاسخ این سئوال در بخش ۴ این مقاله ارائه شده است.
۲. مضامین راهبردی موثر بر معماری کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟ پاسخ به این سئوال در بخش ۵ این مقاله ارائه شده است
۳. اهداف و ماموریت‌های کلان مرتبط با فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟ پاسخ به این سئوال در جدول ۲ ارائه شده است.
۴. فرایندهای کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟پاسخ به این سئوال در جداول ۳ و ۴ ارائه شده است.
۵. ساختار کلان فضای سایبر ج.ا.ا از منظر دفاعی-امنیتی چیست؟ پاسخ به این سئوال در شکل ۳ ارائه شده است.
۶. زیرساخت های فضای سایبر از منظر دفاعی-امنیتی چیست؟ پاسخ به این سئوال در بخش ۷ قسمت زیرساخت های فضای سایبر از منظر دفاعی-امنیتی ارائه شده است.
۷. ارتباطات و تعاملات مولفه های معماری فضای سایبر از منظر دفاعی-امنیتی چیست؟ پاسخ به این سئوال در شکل ۵ ارائه شده است.

پاسخ به سئوال اصلی:

معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی- امنیتی چگونه است؟

مولفه‌های شکل۵ با کیفیتی که در پاسخ به سئوالات فرعی این مقاله آمده است و نحوه تعامل آنها عملاً معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی-امنیتی را تبیین می‌کنند.

وقتی به این معماری از زاویه فرایندها و زیرفرایندهای آن نگاه کنیم متوجه می‌شویم که این معماری در حقیقت ارائه دهنده پنج نظام و زیر نظام‌های مرتبط با آنها در فضای سایبر ج.ا.ا با رویکرد دفاعی-امنیتی نیز هست که منظومه کلان دفاعی-امنیتی ج.ا.ا در فضای سایبر را تشکیل می‌دهند.

این نظام‌ها مستقل از یکدیگر هستند اما منظومه آنها باعث تحقق اهداف کلان ملی از جنبه دفاعی-امنیتی می‌شوند. به عبارت دیگر این نظام‌ها مثل یک تیم فوتبال است که اعضای آنها مستقل هستند و نقش‌های مختلفی مثل دفاع و حمله و غیره دارند ولی همه وقتی نقش خود را به درستی ایفا کنند تیم برنده می‌شود و هرگاه یکی نقش خود را درست اجرا نکند احتمال باخت تیم زیاد می‌شود.

رابطه معماری ارائه شده با معماری جهانی:

لایه حاکمیت سایبر ج.ا.ا ایران که در این کارگروهی معماری شد دقیقا بر همان سه لایه فضای سایبر اعمال می‌شود

که حاکمیت جهانی نیز بر آن اعمال می‌شود و عملاً دو نوع حاکمیت بر این سه لایه اعمال می‌شود. از منظر پنج نظام پدافند، آفند، اطلاعاتی، صیانتی و توانمندسازی اگر به این وضعیت نگاه کنیم سه حالت بین این دو حاکمیت در هریک از این نظامات بصورت جزئی و یا کلی در زیرنظام‌های آنها ایجاد می‌شود که عبارتند از تضاد بین آنها، عدم تضاد و تعامل. حاکمیت ملی مثلاً در زیرنظام امن‌سازی در نظام پدافند ممکن است در لایه خدمات فضای سایبر بخواهد برخی آسیب‌پذیریها را حذف کند در حالیکه این اقدام باعث می‌شود کلاً این خدمت بوسیله حاکمیت جهانی حذف شده و تضاد ایجاد شود. البته در مواردی مثل ایجاد زیرساخت اختصاصی در کشور عدم تضاد وجود دارد و در مواردی مثلا بهربرداری از خدمات جهانی در حوزه‌های علمی در نظام توانمدسازی عملاً بین دو حاکمیت تعامل وجود دارد. استخراج همه این موارد تضاد، عدم تضاد و تعامل کار جداگانه‌ای است که از قلمرو این کارگروهی خارج است ولی تنها راه تدوین راهبردهای مناسب برای دیپلماسی سایبری در جهت تاثیرگذاری بر مذاکرات بین‌المللی به منظور معماری نوین جهانی فضای سایبر خواهد بود.

۹. پیشنهاد:

پیشنهادهای اجرایی:

پیشنهاد می‌شود کمیته‌ای در شورای عالی فضای مجازی تشکیل شود تا با استفاده از این معماری اقدام ذیل را انجام دهد:

بر اساس نظام‌های پیشنهادی در این کار گروهی، نظامات ارائه شده در اسناد راهبردی موجود فضای سایبر ج.ا.ا ایران با رویکرد دفاعی-امنیتی بازبینی شود و تداخلات در نقش نهادها و مواضع مغفول مانده و کیفیت تعامل بین نظامات مذکور بر اساس آنها ارزیابی شود.

پیشنهادهای تحقیقاتی:

- بر اساس الزامات سطح بالای حاصل از نظام‌های مستخرج از معماری پیشنهادی در این پژوهش(مقاله) چهار سند راهبردی پدافندی، آفندی، اطلاعاتی و صیانتی(جرمشناسی با هدف صیانت از امنیت عمومی) برای فضای سایبر کشور با رویکرد دفاعی-امنیتی تدوین شود.
- استخراج موارد تضاد، عدم تضاد و تعامل این معماری با معماری جهانی با هدف روشن کردن موارد حاد دفاعی-امنیتی که در این معماری برای آن چاره‌جویی نشده است و باید مورد توجه بازیگران این حوزه قرار گیرد خصوصاً کسانی که قصد تدوین راهبردهای مناسب برای دیپلماسی سایبری در جهت تاثیرگذاری بر مذاکرات بین‌المللی به منظور معماری نوین جهانی فضای سایبر را دارند.

فهرست منابع ومآخذ

- دولت‌شاه، بهروز، ۱۳۹۵، ارائه الگوی راهبردی در حوزه اقتدار دفاعی- امنیتی بر اساس گفتمان امام و رهبری، قانون اساسی ، تجارب ج.ا.ا. ایران و بهره‌گیری از تجارب موفق بشری ، دانشگاه عالی دفاع ملی

- راه‌نورد غلامعلی، امینی لاری منصور، ۱۳۸۶، چارچوب و متدولوژی سازمان- گرا: ایجاد و توسعه سیستم های اطلاعاتی و معماری سازمانهای گسترده، پنجمین کنفرانس مهندسی صنایع.
- شجاع مودب حمید رضا، ولوی محمد رضا، کریمی قهرودی محمد رضا، حاجی ملامیرزایی حامد، فرحبخت احمد رضا، غریبی جواد، خلیلی علی، مددی آتشگاه حسین، فرزین‌فر منصور، ۱۴۰۰، معماری کلان فضای سایبر ج.ا.ا با رویکرد دفاعی- امنیتی، دانشگاه عالی دفاع ملی
- صالح نیا، علی، ۱۳۹۵، بررسی نظری مفهوم امنیت ملی و ابعاد مختلف آن. مجموعه آثار و مقالات برگزیده دهمین کنگره پیشگامان پیشرفت.
- صنیعی، محمد حسین ، ۱۳۹۵ ، جزوه درس مبانی امنیت ملی، دانشکده امنیت، دانشگاه عالی دفاع ملی
- محمدپور احمد، ۱۳۸۷، ارزیابی کیفیت در تحقیق کیفی :اصول و راهبردهای اعتباریابی و تعمیم‌پذیری، فصلنامه علوم اجتماعی، شماره ۴۸
- مصطفی‌جعفری، سیدکیانوش‌کلانتر بی‌تا ،۱۳۸۳، « معماری سازمان برپایه فناوری اطلاعات و ارتباطات » ماهنامه تدبیر شماره ۱۴۳.
- معینی علی، مراتی احسان، ۱۳۹۴، تدوین روش توسعه چارچوب معماری سازمانی: مطالعه پدیدارشناسی تفسیری ،دانشکده مدیریت دانشگاه تهران، نشریه مدیریت فناوری اطلاعات، دوره ۷ شماره ۱
- نصرت آبادی جمشید، ۱۳۹۸، ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ا. دانشگاه عالی دفاع ملی.
- هلیلی خداداد، ۱۳۹۸ ارائه الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی. دانشگاه عالی دفاع ملی.

- ANDRESS ،JASON و WINTERFELD ،STEVE. ۲۰۱٤, CYBER WARFARE Techniques ،Tactics and Tools for Security Practitioners.
- Shaw، D.S. ۲۰۱۰, what senior military leaders need to know. *strategy research project ،us army war college*.

چیکده انگلیسی:

Macro-architecture of cyberspace of the Islamic Republic of Iran with a defense-security approach

Valavi Mohamad reza ,Shoja moadab hamid reza, Madadi atashgah hosein

Abstract: To deal with the threats of cyberspace in the country, several strategic plans have been developed and announced nevertheless, the country is weak in achieving major national goals in the field of defense-security of cyberspace. Because there is no coordinated and integrated macro-architecture for governance for defense-security of cyberspace in our country Therefore, the main issue of this research is to present such an architecture. The purpose of this group study is to present the macro-architecture of the cyberspace of the Islamic Republic of Iran with a defense-security approach and the main question of the research is what is the macro-architecture of cyberspace of the Islamic Republic of Iran with a defense-security approach? The research method is qualitative. first by referring to scientific articles and documents, we tried to answer the research questions, then by using the focus group method and by using validity and verifiability dynamics criteria such as Credibility, transferability, Dependability and The Confirmability, the results have been evaluated and confirmed. According to the results

of this study, in order to achieve its national goals from the defense-security perspective in the field of cyberspace, the country needs five strategic programs of defense, offensive, intelligence, protection and empowerment. The requirements of each of the mentioned programs are presented in this architecture.
Keywords: Architecture, macro architecture, cyberspace, defense-security