

راهبردهای پدافند غیرعامل الکترونیک راداری در برابر تهدیدات آتی حساسه‌های اطلاعات الکترونیکی دشمن در افق چشم انداز ۱۴۰۴

سید عبدالرحیم موسوی^۱

محمد سپهری^{۲*}

چکیده

دشمن با بکارگیری حساسه‌های پیشرفته اطلاعات الکترونیکی (الینت) در پایگاه‌های مختلف نظامی از هوا، فضا، زمین، دریا و فضای سایبری کلیه فعالیت‌های سامانه‌های راداری آجا را رهگیری، شناسایی و موقعیت‌یابی می‌نماید. هدف اصلی تحقیق، تدوین راهبردهای پدافند غیرعامل الکترونیک راداری آجا در مقابله با تهدیدات رهگیری، شناسایی و موقعیت‌یابی توسط حساسه‌های اطلاعات الکترونیکی (الینت) دشمن می‌باشد. این تحقیق کاربردی-توسعه‌ای، روش تحقیق آمیخته و روش انجام آن موردی-زمینه‌ای می‌باشد. قلمرو زمانی، وضعیت پدافند غیرعامل الکترونیک راداری آجا و تحقیقات مربوط به تهدیدات از پنج سال قبل تاکنون و پیشنهاداتی برای افق ده سال آتی چشم انداز ارتش ۱۴۰۴ می‌باشد. قلمرو مکانی نیروهای آجا می‌باشد. جامعه آماری کلی هفتاد و چهار نفر که تعداد پانزده نفر از این جامعه به عنوان جامعه خیره می‌باشد. با استفاده از روش خبرگی عوامل محیطی (قوت‌ها، ضعف‌ها، تهدیدها و فرصت‌ها) احصاء و با استفاده از ماتریس SWOT جهت تدوین راهبرد و از نرم‌افزارهای تصمیم‌گیری چندمعیاره و نرم‌افزار TOPSIS جهت تجزیه و تحلیل و اولویت‌بندی راهبردها استفاده گردید. در نتیجه پدافند غیرعامل الکترونیک راداری موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی، تسهیل مدیریت بحران و مصون‌سازی سامانه‌های راداری و به عنوان یکی از بهترین راه‌های مقابله با تهدیدات حساسه‌های اطلاعات الکترونیکی (الینت) دشمن می‌باشد.

واژه‌های کلیدی:

پدافند غیرعامل، پدافند غیرعامل الکترونیک راداری، اطلاعات سیگنالی، اطلاعات الکترونیکی، تهدیدهای آتی.

^۱ دانشجوی مدیریت دفاعی دانشگاه افسری امام علی (ع)

^۲ عضو هیئت علمی دانشگاه پدافند هوایی خاتم الانبیاء (ص)

مقدمه

دشمن^۱ با اهداف خاص نظامی، امنیتی و اطلاعاتی کار جمع‌آوری اطلاعات، مراقبت و شناسایی^۲ از سامانه‌های راداری ما را با استفاده از بکارگیری حساسه‌های مختلف جمع‌آوری اطلاعات به خصوص حساسه‌های اطلاعات سیگنالی^۳ در دو بخش حساسه‌های اطلاعات ارتباطی (کامینت)^۴ و حساسه‌های اطلاعات الکترونیکی (الینت)^۵ از زمین، دریا، هوا، فضا و فضای سایبری و از طریق کشورهای همسایه‌ی ایران اقدام به جمع‌آوری اطلاعات راه‌کنشی، عملیاتی و راهبردی می‌نماید. از مهمترین تهدیدات بر علیه سامانه‌های راداری رهگیری، موقعیت‌یابی و شناسایی توسط حساسه‌های اطلاعات الکترونیکی می‌باشد. اقدامات پدافند غیرعامل راداری مهمترین گام در کاهش، عدم رهگیری، گمراه‌سازی و خنثی‌سازی تهدیدات حساسه‌های اطلاعات الکترونیکی آمریکا می‌باشد. بنابراین به منظور افزایش بازدارندگی، کاهش آسیب‌پذیری، ارتقاء پایداری و مصون‌سازی در طیف فرکانس راداری در حساسه‌ها و گیرنده‌های اطلاعات الکترونیکی دشمن، اقدامات پدافند غیرعامل راداری امری لازم و ضروری می‌باشد. به دلیل عدم تدوین راهبردهای این حوزه یک دغدغه و مشکلی اساسی وجود دارد. "مُدُون نبودن راهبردهای پدافند غیرعامل راداری آجا در برابر تهدیدات رهگیری و شناسایی حساسه‌های اطلاعات الکترونیکی (الینت) دشمن" به عنوان مسئله اصلی تحقیق می‌باشد. بنابراین شناخت نقاط قوت، ضعف، فرصت و تهدید پدافند غیرعامل راداری به منظور کاهش و دفع تهدیدات حساسه‌های اطلاعات الکترونیکی آمریکا با بکارگیری اقدامات پدافند غیرعامل راداری امری لازم و ضروری می‌باشد و در صورت عدم شناخت کامل تهدیدات این حوزه، موجب غافل‌گیری راهبردی، رهگیری، کشف و شناسایی بسیار آسان توسط حساسه‌های اطلاعات الکترونیکی آمریکا و بالا رفتن هزینه‌های دفاعی، ضربه‌خوردن از نقاط آسیب‌پذیر در سامانه‌های راداری می‌گردد. بنابراین هدف اصلی تحقیق "تدوین راهبردهای پدافند غیرعامل راداری آجا در مقابله با تهدیدات رهگیری و شناسایی حساسه‌های اطلاعات الکترونیکی آمریکا" و سوال تحقیق "راهبردهای پدافند غیرعامل الکترونیکی سامانه‌های راداری آجا در مقابله با تهدیدات رهگیری و شناسایی حساسه‌های اطلاعات الکترونیکی آمریکا کدامند؟" می‌باشد.

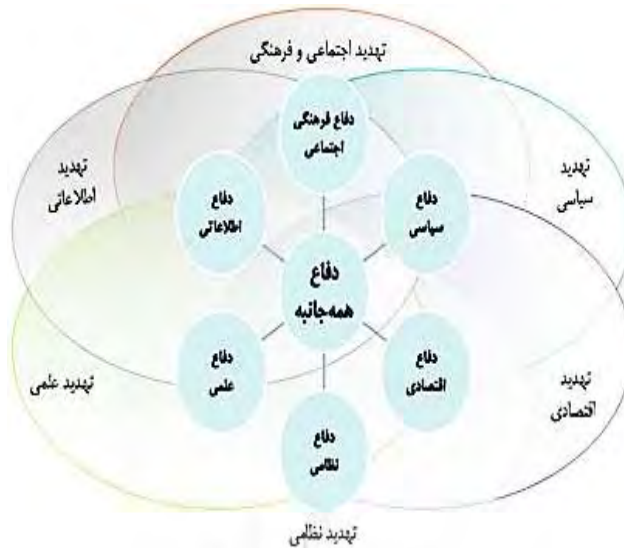
۱. در این مقاله منظور از دشمن فقط آمریکا و تهدیدات حاصل از حساسه‌های اطلاعات الکترونیکی (الینت) می‌باشد.

۲. INFORMATION SURVEILLANCE RECONNAISSANCE (ISR)

۳. SIGNAL INTELLIGENCE (SIGINT)

۴. COMMUNICATION INTELLIGENCE (COMINT)

۵. ELECTRONIC INTELLIGENCE (ELINT)



نمودار (۱) الگوی دفاع همه‌جانبه (بوالحسنی و همکاران، ۱۳۹۵: ۳۳۱)

مبانی نظری و پیشینه پژوهش

الف. نظریه‌های مرتبط با پدافند غیرعامل

۱- نظریه دفاع همه‌جانبه

آماده‌سازی و به‌کارگیری همه سرمایه‌های انسانی، مادی و معنوی به‌منظور پیشگیری و مقابله با هر نوع تهدید و تهاجم دشمنان خارجی و داخلی دفاع همه‌جانبه می‌باشد. دفاع همه‌جانبه به این معناست که امکانات معنوی، فیزیکی، اقتصادی و سایر امکانات ساختار دولتی، دولت‌های محلی، نیروهای دفاعی و کل کشور در یک وضعیت آمادگی مستمر باشند تا یک وضعیت بحران را مهار یا مدیریت کنند و به گونه‌ای یکپارچه عمل نمایند که از خطر یا حمله جلوگیری و کشور را حفظ کنند. در یک نگرش اصولی، برداشت متعارف از انسجام یک کشور، بر توان آن کشور برای آزادی از تسلط یک قدرت خارجی متکی است. در نگاه اولیه، معمولاً حمله به هویت کشور، با نیروی نظامی پاسخ داده می‌شود. با وجود این، تهدیدها نسبت به هویت فقط تهدیدهای فیزیکی نیستند و تهدیدهای فیزیکی نیز فقط از نوع اعلان جنگ نیستند (خانی، ۱۳۷۶: ۱۴۹). امام خمینی^(ع)، برای تولید و بازتولید امنیت در جامعه، مفهوم دفاع همه‌جانبه را مطرح کردند. رویکرد دفاع همه‌جانبه در حقیقت دکترین دفاعی ایران است، که بر اساس آراء و اندیشه‌های امام و مقام معظم رهبری که برگرفته از احکام و فقه اسلام می‌باشد، طراحی شده است. با این رویکرد انقلاب

اسلامی در بیش از سه دهه، توانسته در مقابل انواع تهدیدات و تهاجمات مختلف از جمله جنگ تحمیلی، تحریم‌های اقتصادی و فتنه‌های سیاسی، فرهنگی، اقتصادی و نظامی استکبار جهانی ایستادگی نماید و علاوه بر آن الگوی انقلاب اسلامی را نیز تکثیر و صادر نماید (دری‌نوگورانی، ۱۳۸۷: ۱۱۵).

۲- نظریه دفاع در عمق (دفاع لایه‌ای)

اگرچه دفاع در عمق یا دفاع لایه‌ای و یا دفاع لایه به لایه ابتدا برای امنیت اطلاعات و شبکه مجازی به کار گرفته شد، اما امروزه دفاع در عمق یک راهبرد دفاعی بصورت عام تلقی می‌شود. راهبرد دفاع در عمق همان‌گونه که از نام آن نیز برمی‌آید، یک پدیده راهبردی است و دارای اجزایی است که برهم‌کنش این اجزا این راهبرد را شکل می‌دهد. این اجزا عبارتند از؛ افراد، فناوری و عملیات غفلت از هر یک از این اجزا سبب می‌شود که طراحی و اجرای راهبرد با ناکارآمدی مواجه شود (هادوی، ۱۳۹۱: ۱۳۷). دفاع در عمق یک مدل حفاظتی و لایه‌ای قدرتمند برای اجزای مهم سامانه‌های اطلاعاتی است، یکی از الگوهای دفاعی در آن، دفاع لایه‌ای یا چند لایه است. هدف از دفاع لایه‌ای به کارگیری از چندین سازوکار مراقبت، شناسایی و حفاظت است تا یک مهاجم مجبور به عبور از موانع مختلف بازرسی جهت دستیابی به اطلاعات، حیاتی گردد (پوروهاب، ۱۳۹۳: ۲۷). دفاع در عمق یک راهبرد عمل‌گرایانه برای دستیابی به ایمنی اطلاعات در محیط شبکه محور امروزی است. این راهبرد الگویی است که شدیداً بر کاربرد هوشمندانه فنون و فناوری‌هایی قابل دسترس امروزی تکیه دارد. این راهبرد میان توجه به ظرفیت حفاظت از اطلاعات با توجه به هزینه، عملکرد و ملاحظات عملیاتی توازن برقرار می‌کند (هادوی، ۱۳۹۱: ۱۳۵).

ب. الگوواره‌های (پارادیم‌های) حاکم بر جنگ‌های آتی

جنگ‌های امروزی و آتی در سطوح عملیاتی، راه‌کنشی و راهبردی بر مبنای الگوواره‌های جنگ‌های راهبردی، اطلاعاتی، سایبری، نامتقارن، بدون سرنشین، دانشی، شبکه‌محور، موازی و سایبری می‌باشد. با توجه به گستردگی مختلف تهدیدها در حوزه‌های مختلف از جمله اطلاعاتی، سایبری، الکترونیکی و شبکه محور (سایبرالکترونیک)، دفاع عامل به همراه پدافند غیرعامل امری بسیار لازم و ضروری و مکمل یکدیگر می‌باشد. مناسب‌ترین و بهترین شیوه مقابله در برابر این نوع تهدیدها، پدافند غیرعامل می‌باشد. بنابراین پدافند غیرعامل الکترونیک راداری الگوواره‌ی بسیار

مناسبی جهت کاهش آسیب پذیری، ارتقاء پایداری و مصون سازی سامانه های راداری در برابر تهدیدهای مختلف می باشد (اندیشگاه شریف، ۱۳۸۴: ۸۴).



نمودار (۲) الگو واره ی پدافند غیرعامل الکترونیک راداری (منبع: نظر خبرگان)

ج. مفهوم شناسی

جدول (۱) تعاریف مفاهیم

عنوان	تعریف مفاهیم
پدافند غیرعامل	مجموعه اقدامات غیرمسلحانه ای که موجب، افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می گردد (جلالی، ۱۳۹۱: ۱۳۳).
اطلاعات سیگنالی	جمع آوری اطلاعات از انتشارات الکترومغناطیسی دشمن، رقیب و دوستان در زمان صلح، بحران و جنگ از طریق جستجو، رهگیری، شناسایی، پیاده سازی و موقعیت یابی منبع انتشار انرژی و امواج الکترومغناطیسی که از بخش های اطلاعات الکترونیکی (الینت)، اطلاعات ارتباطی (کامنت) تشکیل شده است (واحدی و همکار، ۱۳۹۰: ۵۲).
اطلاعات الکترونیکی	سیگنال های غیرارتباطی (راداری) دشمن را به منظور تعیین جزئیات سامانه های الکترومغناطیسی دشمن دریافت می کند تا بتواند اقدامات ضدالکترومغناطیسی را برای آنها تدارک ببیند (آدامی، ۱۳۸۵: ۵).

پدافند غیرعامل راداری	اتخاذ روش‌های مناسب، مؤثر و قابل اجرا به منظور افزایش امنیت، ایمنی و پایداری سامانه‌های ارتباطی، غیرارتباطی (راداری) و سایبری (رایانه‌ای) در مقابل حملات ارتباطی، الکترونیکی و سایبری، عملیات شناسایی و جمع‌آوری اطلاعات الکترونیکی دشمن، حذف یا به حداقل رساندن خسارات وارده به توانایی‌های نیروی انسانی، تجهیزات و سامانه‌های الکترونیکی در مقابل اقدامات جمع‌آوری حساسه‌های طیفی، تهاجمات گسترده تجهیزات تخریب الکترومغناطیسی و سایر سامانه‌های مرتبط دشمن با اجرای اصول پدافند غیرعامل می‌باشد (حسنی‌زدری، ۱۳۹۲: ۲۱).
-----------------------------	---

د. پدافند غیرعامل در اسناد بالادستی

مقام معظم رهبری (مدظله‌العالی) می‌فرمایند: «پدافند غیرعامل مثل مصونیت‌سازی برای بدن انسان است، از درون ما را مصون می‌کند. این معنایش این است که ولو دشمن تهاجمی بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد این پدافند غیرعامل نتیجه‌اش این است... ببینید چقدر مهم است که ما این حالت را برای کل پیکره کشور و جامعه در دستگاه‌های مختلف بوجود بیاوریم... کاری کنیم که مصونیت در خودمان بوجود بیاوریم، این با پدافند غیرعامل تحقق پیدا می‌کند. بنابراین این مسئله، مسئله بسیار مهمی است که بایستی راه بیفتد... بنابراین، پدافند غیرعامل یک اصل خواهد بود برای همیشه، نه برای یک مقطع خاص» (www.khamenei.ir، ۹۱/۸/۷). پدافند غیرعامل بطور مستقیم و غیرمستقیم در اسناد بالادستی (منابع دینی، فرمایشات و سخنان حضرت امام خمینی (رحمه‌الله علیه) و فرماندهی معظم کل قوا (مدظله‌العالی)، قانون اساسی، سند چشم‌انداز، سیاست‌های کلی نظام، برنامه چهارم، پنجم، ششم توسعه و سند راهبردی پدافند غیرعامل الکترونیک با نگاه دفاع همه‌جانبه از زیرساخت‌های حیاتی، حساس و مهم (سامانه‌های راداری) در کلیه برنامه‌ها و فعالیت‌ها با رعایت اصول و الزامات پدافند غیرعامل (پدافند غیرعامل راداری) موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران و مصون‌سازی در مقابل تهدیدات حساسه‌های اطلاعات سیگنالی و اقدامات نظامی دشمن می‌شود. ارتقاء مؤلفه‌های اصلی پدافند غیرعامل نیاز به بومی‌سازی، هوشمندسازی، مصون‌سازی فناوری‌های نوین سامانه‌های دفاعی به ویژه سامانه‌های الکترونیکی (راداری)، هوافضایی، دریایی و پدافند هوایی می‌باشد (www.khamenei.ir، ۱۳۹۴/۴/۱۵). فرهنگ‌سازی و ارتقاء سطح آموزش، تحقیقات و فناوری‌های پدافند غیرعامل نیاز به گسترش همکاری‌ها با مراکز علمی دانشگاهی نظامی و غیرنظامی آجا می‌باشد (جلالی و همکار، ۱۳۸۹: ۱۰). برنامه‌ریزی و هدایت پدافند غیرعامل راداری با هدف مصون‌سازی، تضمین تداوم و راهبری ماموریت‌های؛ رصد، پایش، تشخیص، واپایش و هشداردهی تهدیدات حوزه الکترونیک،

مصون سازی و کاهش آسیب پذیری های زیرساخت های الکترونیک آجا در برابر تهدیدات، گفتمان و فرهنگ سازی، تربیت نیروی انسانی مبتکر، متخصص و متعهد، طرح ریزی، آموزش، تجهیز، تمرین، رزمایش و ارزیابی برای ارتقاء آمادگی، طبقه بندی و سطح بندی زیرساخت ها بر اساس اهمیت و ماهیت، ساماندهی، راهبری و حمایت از تحقیق، توسعه و مدیریت دانش کارآمد، در پدافند غیرعامل راداری و ممانعت از دسترسی و بهره برداری دشمن از طیف الکترومغناطیس نیروهای مسلح می باشد (سازمان پدافند غیرعامل الکترونیک کشور، ۱۳۹۵: ۵).

ه. توانمندی های حساسه های اطلاعات الکترونیکی آمریکا

۱. رهگیری، تجزیه و تحلیل و شناسایی پارامترهای راداری توسط حساسه های اطلاعات الکترونیکی آمریکا با استفاده از ۴۱۲۰ پایگاه زمینی، دریایی، هوایی در سطح جهان و ۶۵ پایگاه در همسایگی ایران و فضای سایبری با هدف تسلط کامل بر طیف الکترومغناطیسی (شکوری و همکار، ۱۳۹۴: ۷۶) و توانایی تعیین نوع، تعداد، موقعیت، تحرک، جابجایی، اهداف، قابلیت ها، توانایی ها، نقاط قوت، نقاط ضعف، پیش بینی حمله قریب الوقوع، الگوی فعالیت هر فرستنده، تکنیک و تاکتیک های بکار گرفته شده و تعیین آرایش نظامی الکترونیکی سامانه های راداری توسط حساسه های اطلاعات الکترونیکی (ایزدی، ۱۳۹۳: ۲۳).

۲. استفاده از حساسه های پرفت^۱ اطلاعات سیگنالی زمین پایه در حوزه راه کنشی، عملیاتی و راهبردی در کشورهای همسایه ایران و استفاده از حساسه های اطلاعات سیگنالی هواپایه راه کنشی، عملیاتی و راهبردی هواپیماهای جی استارز، یوتو، GR/CS، RC-۱۳۵ و RC-۱۳۵V، EC-۱۳۰، SR-۷۱، U-۲ و TR-۱، RU-21H و RC-12D، پهپاد گلوبال هاوک، ورهیت^۲، شدو^۳، بالون های PSS2 جمع آوری اطلاعات سیگنالی، حساسه های اطلاعات الکترونیکی فضاپایه (۲۰۰ ماهواره اطلاعات سیگنالی توسط سازمان امنیت ملی). (اسفندیاری و همکاران، ۱۳۸۷: ۱۲۳-۱۴۵).

۳. پشتیبانی اطلاعاتی شانزده سازمان از جمله (سازمان امنیت ملی، آژانس اطلاعات دفاعی، آژانس اطلاعات فضایی، اداره شناسایی ملی، مراکز ذخیره اطلاعات مشترک، فرماندهی امنیت و اطلاعات، آژانس امنیت ملی) تولیدکننده اطلاعات الکترونیکی از فرماندهان نظامی آمریکا و تهیه و تأمین اطلاعات الکترونیکی در حوزه های راه کنشی، عملیاتی و راهبردی.

۴. همگرایی و یکپارچه سازی اطلاعات سیگنالی با جنگ سایبری و جنگ الکترونیک (سایبر

1. PRPHET

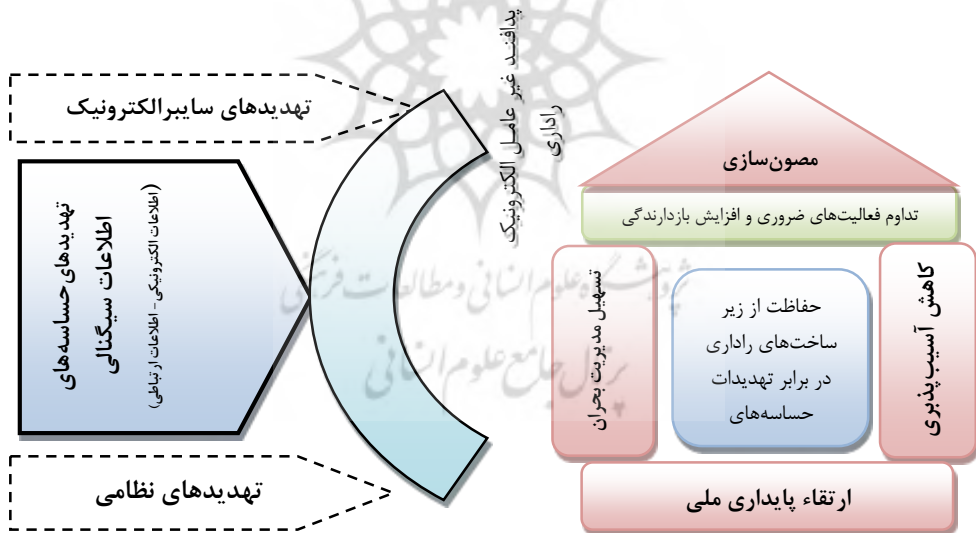
2. VERHEAT

3. SHADW

الکترونیک) (عرفانی و همکاران، ۱۳۹۲: ۸۵-۲۴۳).

و. اقدامات پدافند غیرعامل الکترونیک راداری

بر اساس مطالعه ادبیات تحقیق و نتایج حاصله از مصاحبه و پرسش نامه توزیع شده بین خبرگان جامعه آماری اقدامات پدافند غیرعامل الکترونیک راداری در برابر حساسه های اطلاعات الکترونیکی (الینت)؛ کنترل تشعشعات راداری (مدیریت هوشمند طیف فرکانس)، بدل سازی، شبیه سازی، چندمنظوره سازی و فریب الکترونیکی راداری، پنهان کاری با استفاده از استتار و اختفاء راداری (استتار راداری)، بکارگیری فناوری احتمال رهگیری کم و احتمال آشکارسازی کم راداری (بکارگیری رادارهای غیرفعال، رادارهای دوپایه و چندپایه، آنتن هایی با لوب های جانبی خیلی کم، رادار با سیگنال هایی با پهنای باند خیلی زیاد، توان کم با عرض پالس زیاد، ارسال سیگنال فرستنده به صورت چیرپ، فرکانس تکرار پالس در حالت منظم و تصادفی در رادارها، فشردگی پالس، جابه جایی سریع فرکانس، لوب جانبی پایین و استفاده از آنتن چند پرتوی)، آمایش سامانه های راداری و تحرک و جابجایی سریع سامانه های راداری می باشد.



نمودار (۳) پدافند غیرعامل راداری با توجه به تهدیدات (سپهری: ۱۳۹۶، ۲۱۹)

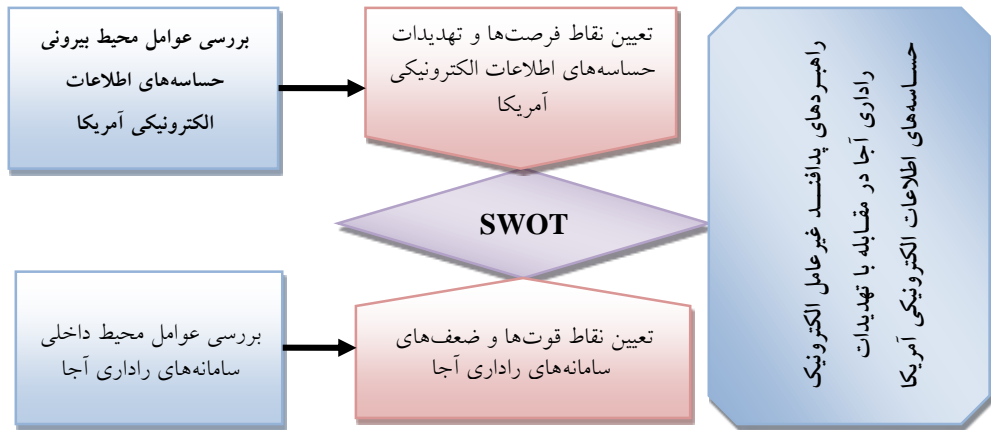
و. کاربردهای سامانه های راداری

رادارهای تهدید غیرمستقیم همانند؛ رادارهای هشداردهنده اولیه، ارتفاع یاب (رادارهای چند بیمه، رادارهای آرایه فازی)، هدف یاب، کنترل رهگیری زمینی، پرکننده شکاف، جستجوگر، هشدار اولیه

هوایی (دهقان پور، ۱۳۸۷: ۹-۶۴)، رادارهای تهدید مستقیم همانند؛ رادارهای کنترل آتش، چند منظوره، آرایه‌ای چند منظوره، ردیاب هدف، ردیاب حین اسکن، رهگیری هوایی، حفاظت از پشت سر هواپیما، نبرد زمینی، کنترل آتش، هدایت موشک، آشکارساز هدف (ستاریخواه و همکاران: ۱۳۸۷: ۵۱-۱۱۳)، رادارهای غیرتهدیدی همانند؛ رادارهای مراقبت فرودگاهی، مراقبت خطوط هوایی، کشف سطح فرودگاهی، تقرب دقیق، مراقبت ثانویه، داپلر هواشناسی، کنترل تقرب زمینی، هواشناسی، اجتناب از طوفان هوایی، کنترل ترافیک هوایی، مراقبت هوایی، داپلر ناوبری، ناوبری، اجتناب از عوارض زمینی (سپهری: ۱۳۹۳: ۲۵-۷۷) و رادارهای با اهداف خاص همانند؛ رادارهای هوانوردی، ترسیم هوایی، کنترل آتش توپخانه، تعقیب زمینی، پهلوگر، تعیین موقعیت خمپاره‌انداز و توپخانه، هوایی، احتمال کم رهگیری، رادار فیوز مخصوص انفجار پرتابه از راه دور، مراقبت ساحلی، موج پیوسته با امواج منقطع شده، ترسیم نقشه زمینی، روزنه‌ی دید ترکیبی، ارتفاع‌سنج، شناسایی دوست از دشمن می‌باشند. (صادق‌نژاد، ۱۳۹۱: ۳۴۳-۷۲۵).

روش‌شناسی پژوهش

این پژوهش از نظر هدف کاربردی، توسعه‌ای و روش تحقیق آمیخته از نوع موردی-زمینه‌ای می‌باشد. روش گردآوری اطلاعات بصورت کتابخانه‌ای و ابزار آن بررسی اسناد و مدارک، آرشیو، کتاب، استفاده از اطلاعات موجود در وبگاه اینترنت، مصاحبه و با استفاده از پرسش‌نامه جهت اخذ نظر خبرگان استفاده شده است. جهت تجزیه و تحلیل و آرایه راهبردها از روش تدوین راهبرد دیوید استفاده شده و با استفاده از روش خبرگی عوامل محیطی (قوت، ضعف، تهدیدها و فرصت‌ها) احصاء و با استفاده از ماتریس SWOT جهت تدوین راهبرد و استفاده از نرم‌افزار TOPSIS در تعیین اولویت راهبردها استفاده شده است. قلمرو زمانی پژوهش از ۵ سال قبل تاکنون خواهد بود و پیشنهاداتی برای افق ۱۰ سال آتی در افق چشم‌انداز ارتش ۱۴۰۴ تا پایداری عوامل محیطی دارد. قلمرو مکانی آجا می‌باشد. جامعه آماری ۷۴ نفر تمام شمار، که دارای حداقل ۱۵ سال سابقه اجرایی و دارای مدرک تحصیلی ۶۸ درصد دکتری و ۳۲ درصد کارشناسی ارشد می‌باشد. روایی پرسش‌نامه به تایید خبرگان و اساتید دانشگاهی رسیده و پایایی آن با استفاده از آزمون آلفای کرونباخ ۰/۸۸ بوده که نشانگر پایایی پرسش‌نامه می‌باشد. در ادامه در نمودار (۴) مدل مفهومی پژوهش ارائه شده است.



نمودار (۴) مدل مفهومی پژوهش (منبع: محقق ساخته)

تجزیه و تحلیل یافته‌ها

الف- شناسایی و استخراج عوامل محیطی داخلی و خارجی

به منظور شناسایی عوامل محیطی ابتدا مطالعات اکتشافی و بررسی اسناد، مدارک و اسناد بالادستی صورت گرفته و پس از احصاء عوامل اولیه در جلسات تخصصی و نشست‌های خبرگی و طوفان مغزی عوامل داخلی از خارجی به تأیید جامعه خبره رسید. پس از آن این عوامل در دو بخش داخلی و خارجی در قالب پرسشنامه جهت کسب نظر جامعه آماری ارائه و با توجه به حجم جامعه آماری و پارامترهای توصیفی، عوامل چهارگانه محیط داخل و خارج و وضع موجود این عوامل مشخص و پس از جمع‌آوری پاسخ‌ها، نتایج و جمع‌بندی آنها به شرح ذیل می‌باشد:

۱- ماتریس ارزیابی عوامل خارجی (EFE)

نتایج حاصل از پرسش‌نامه توزیع شده در بین جامعه آماری عبارتند از:

جدول (۲) محاسبه فرصت‌های پدافند غیرعامل راداری

نمره موزون	وزن موجود (اهمیت)			نقاط فرصت
	ضریب اهمیت	وزن	میانگین	
۰/۱۴۳۶	۲/۸۷۸	۰/۰۴۹۹	۸۲/۱۸۹۲	۱- استفاده از توان علمی دانشگاه‌های نظامی و غیرنظامی کشور در طراحی، ساخت، بکارگیری و مهندسی معکوس سامانه‌های راداری مجهز به فناوری‌های پدافند غیرعامل راداری و حفاظت الکترونیکی بومی.

۰/۱۷۹۸	۳/۴۳۲	۰/۰۵۲۴	۸۶/۳۳۷۸	۲- بکارگیری رادارهای غیرعامل، دویایه و چندپایه با هدف کاهش و عدم رهگیری توسط حساسه‌های اطلاعات الکترونیکی آمریکا.
۰/۱۸۴۱	۳/۵۲۷	۰/۰۵۲۲	۸۵/۸۹۱۹	۳- بکارگیری سامانه فرماندهی و کنترل هوشمند بومی با هدف هماهنگی و یکپارچگی فعالیت‌های سامانه‌های راداری.
۰/۱۶۷۵	۳/۳۷۸	۰/۰۴۹۶	۸۱/۷۱۸۲	۴- بکارگیری مؤثر شبکه‌های ارتباطی فیبرنوری، رمزهای پیشرفته و هوشمند بومی در سامانه‌های ارتباطی و سایبری مورد استفاده در سامانه‌های راداری.
۰/۱۵۴۸	۳/۱۳۵	۰/۰۴۹۴	۸۱/۰۶۷۶	۵- تشخیص، رفتارشناسی و آمایش سرزمینی (هوایی، زمینی، دریایی و فضایی و سایبری) حساسه‌های اطلاعات الکترونیکی آمریکا در منطقه.
۰/۱۵۷۲	۳/۱۰۸	۰/۰۵۰۶	۸۳/۳۹۱۹	۶- بکارگیری انواع سامانه‌های کاذب و فریب راداری با هدف انحراف و گمراه‌سازی حساسه‌های اطلاعات الکترونیکی آمریکا.
۰/۱۵۲۸	۳/۰۹۵	۰/۰۴۹۴	۸۱/۴۷۳۰	۷- تحرک، جابجایی بسیار سریع، ایجاد فاصله بین فرستنده و گیرنده سامانه‌های راداری.
۰/۱۴۶۷	۲/۹۴۶	۰/۰۴۹۸	۸۲/۰۴۰۵	۸- استفاده از سازه‌های فنی در سامانه‌های راداری.
۰/۱۵۳۱	۳/۰۱۴	۰/۰۵۰۸	۸۳/۵۵۴۰	۹- بکارگیری فناوری احتمال رهگیری، کشف کم ^۱ بکارگیری و مدیریت توان بومی در سامانه‌های راداری.
۰/۱۴۲۱	۲/۸۶۵	۰/۰۴۹۶	۸۱/۷۴۳۲	۱۰- بکارگیری فناوری مدیریت توان و کنترل انتشارات امواج راداری.
۱/۵۸۱۷	۳۱/۳۷۸	۰/۵۰۳۷	۸۲۹/۴۰۵۳	جمع

جدول (۳) محاسبه تهدیدهای پدافند غیرعامل راداری

نمره موزون	وزن موجود (اهمیت)			نقاط تهدید
	ضریب اهمیت	وزن	میانگین	
۰/۱۸۴۹	۳/۶۷۶	۰/۰۵۰۳	۸۲/۸۳۷۸	۱- دستیابی سریع به آرایش نظامی الکترونیکی و آمایش سرزمینی سامانه‌های راداری توسط حساسه‌های اطلاعات سیگنالی آمریکا.
۰/۲۰۸۲	۴/۲۱۶	۰/۰۴۹۴	۸۱/۴۱۸۹	۲- استفاده از پایگاه هوایی، زمینی، دریایی و فضای آشکار و پنهان جمع‌آوری اطلاعات الکترونیکی آمریکا در همسایگی ایران.
۰/۲۱۲۹	۴/۲۴۳	۰/۰۵۰۲	۸۲/۵۰۰۰	۳- توانایی استفاده از سکوه‌های فضاپایه جمع‌آوری اطلاعات الکترونیکی (ماهواره‌های چالت، ورتکس، ماگنوم و...) در رهگیری و شناسایی سامانه‌های راداری.

^۱. LOW PROBABILITY OF INTERCEPT/ LOW PROBABILITY OF DETECTION (LPI/ LPD)

۰/۲۱۴۶	۴/۳۱۱	۰/۰۴۹۸	۸۲/۱۲۱۶	۴- توانایی بهره‌برداری از سکوه‌های جمع‌آوری اطلاعات الکترونیکی و شناسایی هوایی (RC-۱۳۵) و پهپادهای پریدیتور، گلوبال‌هاک، دارک استار و ...
۰/۲۱۱۲	۴/۲۸۴	۰/۰۴۹۳	۸۱/۲۸۳۸	۵- توانایی استفاده از سکوه‌های دریایا به سطحی و زیرسطحی جمع‌آوری اطلاعات الکترونیکی جهت رهگیری سامانه‌های راداری در منطقه خلیج فارس و دریای عمان.
۰/۲۲۱۳	۴/۳۹۲	۰/۰۵۰۴	۸۳/۰۴۰۵	۶- استفاده از فرماندهی اطلاعات و امنیت در کنار سایر سازمان‌های اطلاعاتی آمریکا.
۰/۲۰۷۸	۴/۲۱۶	۰/۰۴۹۳	۸۱/۰۱۳۵	۷- توانایی رهگیری، تجزیه و تحلیل، شناسایی، موقعیت‌یابی کلیه سامانه‌های راداری توسط حساسه‌های هوشمند جمع‌آوری اطلاعات الکترونیکی از هوا، زمین، دریا، فضا و فضای سایبر.
۰/۲۲۰۴	۴/۳۶۵	۰/۰۵۰۵	۸۳/۱۷۵۷	۸- همگرایی جنگ سایبری، جنگ الکترونیک و اطلاعات سیگنالی (سایبرالکترونیک) آمریکا با هدف تسلط بر طیف الکترومغناطیس.
۰/۲۱۵۷	۴/۳۲۴	۰/۰۴۹۹	۸۲/۲۱۵۶	۹- توانمندی‌های عملیات اطلاعات سیگنالی آمریکا در رهگیری، شناسایی و موقعیت‌یابی بسیار سریع سامانه‌های راداری.
۰/۱۸۹۴	۴/۰۱۴	۰/۰۲۲۹	۷۷/۵۶۷۶	۱۰- تحریم‌های تجهیزاتی، قطعات الکترونیکی و فناوری‌های خاص سامانه‌های راداری توسط آمریکا
۲/۰۸۶۴	۴۲/۰۴۱	۰/۴۹۶۳	۸۱۷/۱۸۹۱	جمع
۳/۶۶۸۱	۷۳/۴۱۹	۱	۱۶۴۶/۵۹۴۴	جمع کل فرصت‌ها و تهدیدها

چون عدد تهدیدات بیش از عدد فرصت‌هاست، بنابراین سامانه‌های راداری در برابر تهدیدات حساسه‌های اطلاعات الکترونیکی (الینت) در محیط خارجی با تهدیدات فناورانه در رهگیری، شناسایی و موقعیت‌یابی روبرو است.

۲- ماتریس ارزیابی عوامل داخلی (IFE)

نتایج حاصل از پرسش‌نامه توزیع شده در بین جامعه آماری عبارتند از:

جدول (۴) محاسبه قوت‌های پدافند غیرعامل راداری

نمره موزون	وزن موجود (اهمیت)			نقاط قوت
	ضریب اهمیت	وزن	میانگین	
۰/۱۶۳۰	۳/۴۳۲	۰/۰۴۷۵	۷۸/۸۵۱۴	۱. بکارگیری الگوهای پدافند غیرعامل از منظر قرآن کریم، آموزه‌های دینی، فرمایشات حضرت امام ^(ره) و مقام معظم رهبری ^(مدظله العالی)

۰/۱۷۴۳	۳/۵۹۴	۰/۰۴۸۵	۸۰/۵۴۰۵	۲. وجود اسناد بالادستی (اصل‌های ۳، ۹ و ۱۷۶ قانون اساسی و برنامه‌های چهارم، پنجم و ششم توسعه کشور و سیاست‌های ابلاغی پدافند غیرعامل توسط مقام معظم رهبری (مدظله العالی) و سند پدافند الکترونیک کشور.
۰/۱۶۸۹	۳/۳۶۴	۰/۰۵۰۲	۸۳/۴۳۲۴	۳. آموزش‌های آکادمیک به کارکنان سامانه‌های راداری کشور با استفاده از توان علمی دانشگاه‌های نظامی و غیرنظامی نسبت به تهدیدات حساسه‌های اطلاعات الکترونیکی آمریکا.
۰/۱۶۲۵	۳/۳۲۴	۰/۰۴۸۹	۸۱/۳۲۴۳	۴. طراحی، ساخت، بکارگیری و مهندسی معکوس سامانه‌های راداری مجهز به فناوری‌های پدافند غیرعامل راداری و حفاظت الکترونیکی بومی با استفاده از توان علمی آجا، دانشگاه‌های نظامی و غیرنظامی و صنایع داخلی (وزارت دفاع و شرکت‌های دانش‌بنیان).
۰/۱۵۶۸	۳/۱۶۲	۰/۰۴۹۶	۸۲/۳۲۴۳	۵. طرح‌ریزی، اجرا و آمایش سرزمینی مناسب سامانه‌های راداری در سطوح عملیاتی، تاکتیکی و راهبردی با رعایت اقدامات و الزامات پدافند غیرعامل راداری بومی.
۰/۱۷۳۶	۳/۴۸۶	۰/۰۴۹۸	۸۲/۸۵۱۴	۶. بکارگیری فرماندهی و کنترل بومی در سامانه‌های راداری.
۰/۱۶۲۸	۳/۲۸۳	۰/۰۴۹۶	۸۲/۴۳۲۴	۷. استقلال و خودکفایی حداکثری در شبکه‌ی یکپارچه راداری.
۰/۱۶۵۲	۳/۳۵۱	۰/۰۴۹۳	۸۲/۵۴۰	۸. بکارگیری اقدامات پدافند غیرعامل راداری از جمله استتار، اختفاء، فریب.
۰/۱۵۸۲	۳/۲۲۹	۰/۰۴۹۰	۸۱/۵۵۴۱	۹. بکارگیری سامانه‌های راداری متحرک تاکتیکی با قدرت تحرک و جابه‌جایی بالا.
۰/۱۵۹۵	۳/۲۴۳	۰/۰۴۹۲	۸۱/۸۹۱۹	۱۰. بکارگیری فناوری‌های حفاظت الکترونیکی راداری (مدیریت توان و کنترل تشعشعات، کنترل زمان حساسیت، پایداری زمان در عرض پالس، جابه‌جایی سریع فرکانس، پالس متراکم، کنترل تشعشعات، رادارهای غیرعامل ^۱ و ...)
۱/۶۴۴۸	۳۳/۴۶۸	۰/۴۹۱۶	۸۱۷/۲۵۶۷	جمع

جدول (۵) محاسبه ضعف‌های پدافند غیرعامل راداری

نمره موزون	وزن موجود (اهمیت)			نقاط ضعف
	ضریب اهمیت	وزن	میانگین	
۰/۳۱۴۴	۴/۱۰۸۱	۰/۰۵۲۲	۸۶/۶۸۹۱	۱. به روز نبودن سامانه‌ها، آموزش و فناوری‌های پدافند غیرعامل راداری و حفاظت الکترونیکی سامانه‌های راداری.
۰/۳۰۶۱	۴/۱۴۸۶	۰/۰۴۹۷	۸۲/۵۸۱۱	۲. مدون نبودن راهبردهای پدافند غیرعامل الکترونیک راداری.

^۱. PASSIVE

۰/۲۰۷۹	۴/۰۵۴۰	۰/۰۵۱۳	۸۵/۱۸۹۱	۳. کفایت نداشتن الزامات پدافند غیرعامل الکترونیک راداری در طراحی، خرید و بکارگیری.
۰/۱۹۸۵	۳/۹۸۶۴	۰/۰۴۹۸	۸۲/۷۸۳۷	۴. کفایت نداشتن فناوری‌های مدیریت توان بومی در طیف الکترومغناطیسی به منظور کنترل انتشارات راداری.
۰/۲۰۷۰	۴/۱۰۸۱	۰/۰۵۰۴	۸۳/۹۳۲۴	۵. کفایت نداشتن سامانه‌های راداری هوای با برد بلند پروازی و قدرت تحرک و جابجایی بسیار بالا.
۰/۲۱۲۳	۴/۲۲۹۷	۰/۰۵۰۲	۸۳/۳۲۴۳	۶. کفایت نداشتن استفاده از رادارهای دو پایه، چندپایه و رادارهای غیرعامل.
۰/۲۱۹۰	۴/۲۲۹۷	۰/۰۵۱۸	۸۶/۱۶۲۱	۷. کفایت نداشتن بکارگیری فناوری احتمال رهگیری و شناسایی کم راداری.
۰/۲۱۸۰	۴/۲۸۳۷	۰/۰۵۰۹	۸۴/۷۵۶۷	۸. کفایت نداشتن فناوری‌های پدافند غیرعامل الکترونیک و حفاظت الکترونیک راداری.
۰/۲۱۴۴	۴/۱۸۹۱	۰/۰۵۱۲	۸۴/۸۵۱۳	۹. کفایت نداشتن دانش و فناوری‌های نوین و پیشرفته پدافند غیرعامل راداری.
۰/۲۱۴۶	۴/۲۱۶۲	۰/۰۵۰۹	۸۴/۷۲۹۷	۱۰. قدیمی بودن وضعیت آمایش سرزمینی سامانه‌های راداری و افشای موقعیت آنها.
۲/۱۱۲۲	۴۱/۵۵۳۶	۰/۵۰۸۴	۸۴۴/۹۹۹	جمع
۳/۷۵۷۰	۷۵/۰۲۱۶	۱	۱۶۶۲/۲۵	جمع کل قوت‌ها و ضعف‌ها

چون عدد ضعف‌ها بیش از مقدار عدد قوت‌ها می‌باشد، بنابراین به این معنی است که پدافند غیرعامل راداری در محیط داخلی با ضعف‌های فناورانه‌ای در طراحی ساخت و بکارگیری روبرو می‌باشد.

پژوهشگاه علوم انسانی و مطالعات فرهنگی

ب- ماتریس ارزیابی موقعیت و اقدام راهبردی علوم انسانی

جهت تعیین موقعیت راهبردی و تحلیل شکاف از ماتریس IFE & EFE بدین صورت استفاده شده است:

$$A = 1.64482 - 2.1122 = -0.46738$$

نمره موزون ضعف‌ها - نمره موزون قوت‌ها = A

$$B = 1.5817 - 2.0864 = -0.5047$$

نمره موزون تهدیدات - نمره موزون فرصت‌ها = B

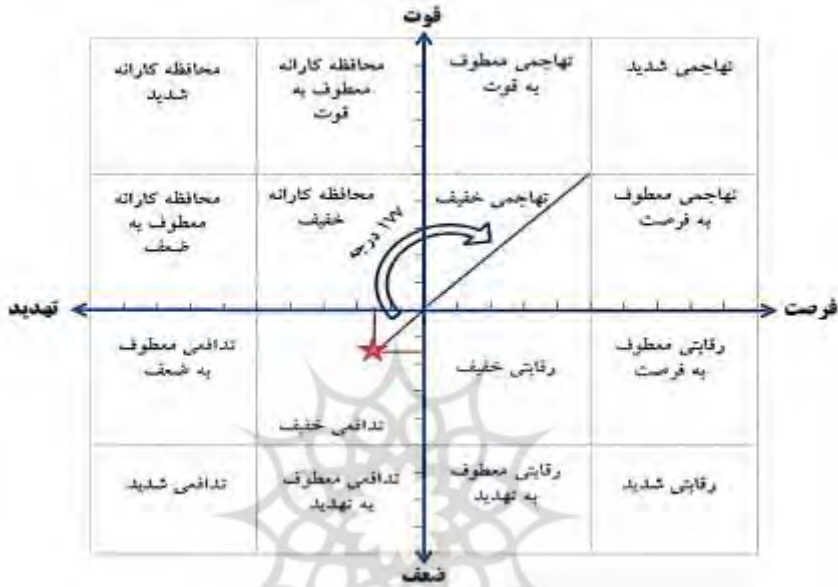
$$C = \text{Arctg } A/B = 42.8^\circ$$

¹. Strategic Position And Action Evaluation Matrix (SPACE)

45° = زاویه نقطه مطلوب (ایده‌آل) با محور X ها

مقدار زاویه چرخش راهبردی از وضع موجود به سمت وضع مطلوب = CD

$$177.8^\circ = 45^\circ, 90^\circ, 42^\circ$$



نمودار (۵) تعیین موقعیت راهبردی

مقدار زاویه چرخش از وضع موجود به وضع مطلوب برابر با 177.8° درجه می‌باشد. وضع موجود پدافند غیرعامل راداری در ناحیه تدافعی یا انفعالی خفیف قرار داشته و تا حدودی تهدید محور است و در وضعیت ناپایداری قرار داشته و در مواجهه با تهدیدها آسیب‌پذیر می‌باشد و از نظر منابع و امکانات تخصصی با مشکل مواجه است و تاکید بر دستیابی به سامانه‌های نوین و هوشمند پدافند غیرعامل الکترونیک راداری با رویکرد راه‌کارهای ناهم‌تراز و میانبر و خلاقانه مدنظر می‌باشد. بنابراین برای رسیدن به وضع مطلوب باید به رویکرد مقتدرانه آموزش، تحقیق، توسعه و تولید پدافند غیرعامل الکترونیک هوشمند و بومی در سامانه‌های راداری با فناوری‌های نوین به رویکرد تهاجمی یا فعال رسیده، به فرصت‌ها توجه بیشتری از قوت‌ها و به نقاط ضعف و قوت داخلی توجه بیشتری شود. در نتیجه پدافند غیرعامل راداری به وضعیت پایدار و مطلوبی خواهد رسید. از این‌رو ضروری است برای رسیدن به نقطه مطلوب، امکانات، تقسیم‌بندی و تخصیص منابع مطابق جدول ذیل صورت پذیرد:

جدول (۶) تقسیم‌بندی و تخصیص منابع

عوامل / درصد منابع تخصیص یافته	مقادیر
قوت	۱/۶۴۵
ضعف	۲/۱۱
فرصت	۱/۵۸
تهدید	۲/۰۹
مجموع قوت و ضعف	۳/۷۵۵
مجموع فرصت و تهدید	۳/۶۷
زاویه بین دو پاره خط	۱۷۷/۸
درصد منابع موردنیاز قوت و ضعف	۵۰/۵۷
درصد منابع موردنیاز فرصت و تهدید	۴۹/۴۳
درصد منابع موردنیاز جهت ارتقای قوت	۲۲/۱۵
درصد منابع موردنیاز جهت رفع ضعف	۲۸/۴۲
درصد منابع موردنیاز جهت به کارگیری فرصت	۲۱/۲۸
درصد منابع موردنیاز جهت دفع تهدید	۲۸/۱۵

نتیجه‌گیری و پیشنهادها

در پاسخ به سوال اصلی تحقیق، راهبرهای ذیل با استفاده از نظر ۱۵ نفر خبره و نرم‌افزار TOPSIS به شرح ذیل رتبه‌بندی گردیده است:

جدول (۷) اولویت‌بندی و مطلوبیت راهبردهای آتی پدافند غیرعامل الکترونیک راداری

اولویت	رتبه	مطلوبیت راهبردها	راهبردها
۱	رتبه اول	۰/۶۲۹	بومی‌سازی اقدامات و الزامات پدافند غیرعامل راداری با هدف مصون‌سازی از طریق طراحی، ساخت و بکارگیری سامانه‌های راداری بومی.
۲	رتبه دوم	۰/۵۷۸	مدیریت هوشمند طیف فرکانس راداری با هدف کنترل تشعشعات از طریق بکارگیری رادارهای آرایه فازی.
۳	رتبه سوم	۰/۵۶۴	متحرک‌سازی سامانه‌های راداری با هدف قدرت تحرک و جابجایی بسیار بالا از طریق بکارگیری رادارهای راه‌کنشی و راهبردی هوایی، زمینی و دریایی.

۴	راهبرد ۲	۰/۱۵۵۸	استتار، اختفاء و پنهان‌کاری سیگنال‌های راداری با هدف دشواری و کاهش رهگیری و شناسایی توسط حساسه‌های اطلاعات الکترونیکی از طریق بکارگیری طریف بکارگیری فناوری‌های احتمال رهگیری و آشکارسازی کم راداری.
۵	راهبرد ۳	۰/۱۵۵۳	غیرعامل نمودن فناوری‌های راداری با هدف کاهش اثر ردیابی توسط حساسه‌های اطلاعات الکترونیکی با استفاده از بکارگیری رادارهای دوطایه، چندپایه.
۶	راهبرد ۴	۰/۱۵۲۹	فریب الکترونیکی حساسه‌های اطلاعات الکترونیکی با هدف بدل‌سازی، شبیه‌سازی و چندمنظوره‌سازی سامانه‌های راداری با استفاده از استتار، اختفاء و آمایش الکترونیکی سامانه‌های راداری.
۷	راهبرد ۵	۰/۱۵۲۷	همگرایی و هم‌افزایی کلیه سامانه‌های فرماندهی و کنترل کشور با هدف کنترل تهدیدات از طریف مدیریت یکپارچه در شرایط صلح، بحران و جنگ.
۸	راهبرد ۶	۰/۱۵۱۶	آموزش تخصصی پدافند غیرعامل راداری با هدف ارتقاء سطح آمادگی رزمی و قدرت پاسخگویی به تهدیدات حساسه‌های اطلاعات الکترونیکی دشمن از طریق اجرای رزمایشات تخصصی.

- با توجه به عوامل احصاء شده و راهبردهای تدوین شده در این پژوهش، پیشنهادات اجرایی پدافند غیرعامل الکترونیک راداری ذیل جهت اقدامات آتی ارائه می‌گردد:
- اصلاح ساختار سازمانی پدافند غیرعامل الکترونیک سامانه‌های راداری.
 - آموزش و نهادینه‌سازی اصول و الزامات پدافند غیرعامل الکترونیک راداری از طریق دانشگاه‌ها و سایر مراکز آموزشی.
 - ارتقاء جایگاه پدافند غیرعامل الکترونیک راداری در کنار پدافند عامل.
 - هم‌افزایی و کاهش هزینه‌ها در طرح‌های ایمن‌سازی حوزه‌های پدافند غیرعامل.
 - اجرای طرح آمایش نوین جهت توسعه طرح‌های آینده سامانه‌های راداری.
 - بکارگیری سامانه‌های راداری غیرعامل در طرح‌های آمایش نوین سامانه‌های راداری.
 - استفاده از فناوری‌های احتمال رهگیری و شناسایی کم در سامانه‌های راداری.
 - بکارگیری فناوری‌های استتار، اختفاء و فریب الکترونیکی در سامانه‌های راداری.
 - مصون‌سازی سامانه‌های راداری با بکارگیری اصول، اقدامات و الزامات پدافند غیرعامل الکترونیک راداری.
 - بکارگیری فرماندهی و کنترل هوشمند بومی در سامانه‌های راداری.

منابع

- آدامی، دیدوید. (۱۳۸۵). جنگ الکترونیک. ترجمه: نایبی، محمد مهدی. و حرمتی، علی. تهران: انتشارات دانشگاه صنعتی شریف.
- ایزدی، پیروز. (۱۳۹۳). اطلاعات نظامی. تهران: دانشکده فرمانده و ستاد سپاه پاسداران انقلاب اسلامی.
- بوالحسنی، خسرو. دری نوگورانی، حسین. بختیاری، ایرج. و سپهری، محمد. (۱۳۹۵). مجموعه مقالات اقتصاد مقاومتی، جلد سوم. تهران. انتشارات دانشگاه عالی دفاع ملی.
- جلالی فراهانی، غلامرضا. (۱۳۹۱). مقدمه‌ای بر مبانی نظری پدافند غیرعامل با رویکرد تهدیدات جدید. تهران: انتشارات دانشگاه امام حسین (علیه‌السلام).
- جلالی فراهانی، غلامرضا. هاشمی فشارکی، سیدجواد. (۱۳۸۹). پدافند غیرعامل در آیینة قوانین و مقررات. تهران: سازمان پدافند غیر عامل.
- جلالی، غلامرضا. (۱۳۹۱). چهار گفتار در باب پدافند غیرعامل. تهران: نشر محدث.
- حسنی‌اژدری، سید مجید. (۱۳۹۲). پدافند غیرعامل ارتباطی و الکترونیکی. نوشهر: انتشارات دانشگاه علوم دریایی امام خمینی (رحمه‌الله‌علیه).
- دهقان‌پور، مهدی. (۱۳۸۳). بررسی انواع رادارها و کاربردهای آن (پایان‌نامه). تهران: دانشگاه هوایی شهید ستاری.
- رزمخواه، محمدرضا. اسفندیاری، مسعود. و سپهری، محمد. (۱۳۸۷). بررسی تطبیقی و پایش تهدیدات فناوری‌های جنگ الکترونیک هوایی و تراز یابی توان فناوری‌های جنگ الکترونیک هوایی دو کشور ایران و آمریکا و آرایه‌ی الگوی تحلیلی مناسب و استخراج فناوری‌ها و تجهیزات جنگ الکترونیک هوایی ایران و مستندسازی آن‌ها، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- سازمان پدافند غیرعامل کشور. (۱۳۹۵). سند راهبردی پدافند غیرعامل الکترونیک کشور. تهران.
- سپهری، محمد. (۱۳۹۶). راهبردهای پدافند غیرعامل سامانه‌های ارتباطی و راداری آجا در مقابله با تهدیدات ناهم‌تراز، از ناحیه‌ی حساسه‌های اطلاعات سیگنالی دشمن، رساله دکتری دانشگاه عالی دفاع ملی.
- سپهری، محمد. و پورابراهیم، علیرضا. (۱۳۹۳). دفاع سایبری در برابر شبکه جمع‌آوری اطلاعات اشلون. دومین کنفرانس دفاع سایبری، دانشگاه جامع امام حسین (علیه‌السلام).
- ستاری‌خواه، علی. (۱۳۸۱). بررسی و شناسایی عوامل اثرگذار بر سامانه جنگ‌های الکترونیکی و تدوین استراتژی جنگ الکترونیک آجا، رساله دکتری دانشگاه عالی دفاع ملی.
- ستاری‌خواه، علی. (۱۳۸۷). جمع‌آوری، تجزیه و تحلیل و پردازش اطلاعات سامانه‌های راداری ارتش آمریکا مستقر در خلیج فارس. تهران: شرکت جلوه‌ی صنعت.

- شکوری، عزیز. و سپهری، محمد. (۱۳۹۴). مدیریت و هدایت اطلاعات سیگنالی. تهران: انتشارات دانشگاه هوایی.
- صادق‌نژاد، احمد. و حیدری، حسین. (۱۳۹۱). آشنایی با سامانه‌های راداری جلد (۱ و ۲). تهران: انتشارات نهجا.
- عرفانی، اسماعیل. حسینی، سید احمد. و سعیدآوی، جبار. (۱۳۹۲). جمع‌آوری، تجزیه و تحلیل و پردازش اطلاعات سامانه‌های جنگ الکترونیک ارتش آمریکا مستقر در خلیج فارس. تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- لونی، محمدرضا. (۱۳۹۱). تدوین راهبرد ملی پدافند غیرعامل در حوزه ارتباطات، تهران: دانشگاه عالی دفاع ملی.
- WWW://farsi.khamenei.ir/91/7/8.
- Rhoes, J. E. (1999). Signals Intelligence MCWP 2-15.2-U.S. Marine Corps.

