

## مقاله پژوهشی: ارائه راهبردهای ارتقاء قدرت هوایی پرنده های بدون سرنشین راهبردی (پهپاد) در برابر تهدیدات هوای پرنده های بدون سرنشین

هادی باغبانی<sup>۱</sup>

دریافت مقاله: ۱۴۰۳/۰۲/۱۷

پذیرش مقاله: ۱۴۰۳/۰۳/۲۸

### چکیده

از آنجا که انواع پرنده های بدون سرنشین کشور در بعد سوم جنگ ( قدرت هوایی ) به عنوان سرمایه ملی محسوب می گردند بررسی وضعیت آن ها و میزان آسیب پذیری در مقابله با انواع تهدیدات هوایی قابل شناسایی محتمل اعم از سامانه های کنترل و فرماندهی پرنده ها، جنگنده های نسل چهارم و پنجم موجود در اختیار کشورهای فرامنطقه ایی و منطقه ایی به صورت ملموس جهت شناسایی راداری و انواع سنجنده منصوب بر روی سامانه های یاد شده دشمن ( اعم از هوایی و زمینی ) محسوب می گردند. هدف پژوهش حاضر کاهش آسیب پذیری در برابر تهدیدات هوایی پرنده های بدون سرنشین به عنوان مکمل پرنده های با سرنشین (قبل از پرواز، حین پرواز و هنگام فرود) به منظور ارتقاء توان رزم حوزه هوایی بود. روش پژوهش آمیخته از نوع موردی-زمینه ای و روش تحلیلی بود. جامعه آماری پژوهش حاضر را کلیه خبرگان حوزه ی هوایی نیروهای مسلح و مراکز علمی تشکیل داده بودند. برای تعیین حجم نمونه از جدول مورگان استفاده شد که در نهایت ۳۶۰ نفر با استفاده از روش نمونه گیری در دسترس انتخاب شدند. روش تحلیل داده ها به شیوه کیفی (استدلالی) و کمی (توصیفی و استنباطی) با استفاده از نرم افزار SPSS و بهره گیری از محیط EXCEL انجام پذیرفته است. یافته های به دست آمده نشان داد که چون مقدار آماره آزمون Z از مقدار بحرانی بزرگ تر است؛ بنابراین اهداف پژوهش مورد تایید قرار م گیرند ( $p=0/05$ ). به نظر می رسد که برنامه ریزی اجرایی و اولویت بندی نتایج مستخرجه از نتایج اهداف سه گانه (قبل از پرواز، حین پرواز، هنگام فرود) مهم و ضروری می باشد.

**واژگان کلیدی:** پرنده های بدون سرنشین (پهپاد)، تهدید، تهدیدات هوایی، ارتقاء قدرت هوایی

۱ هادی باغبانی، استادیار مدیریت راهبردی (پدافند غیرعامل) دانشگاه علوم و فنون هوایی شهید ستاری

**مقدمه**

طرح‌ریزی عملیات نظامی در عصر جنگ‌های مدرن به اقدامی بس دشوار و تخصصی بدل گردیده است که لازمه آن شناخت چند بعدی مولفه‌های موثر در جنگ و توان جانمایی و ارائه معماری دقیق از عوامل موثر برتر ساز صحنه نبرد است. (پیوند، ۱۴۰۱: ۱) با توجه به تغییرات نظامند جنگ‌های اخیر و آینده و نقش ارزنده نیازمندی به بهره مندی از پهپاد در بعد سوم جنگ ( قدرت هوایی ) به عنوان سرمایه ملی محسوب می‌گردند.

پرنده‌های هدایت‌پذیر از دور (پهپاد) چه مسلح و چه غیرمسلح، نقش مهمی را در این تحول و انقلاب تسلیحاتی بازی می‌کنند؛ زیرا این سامانه‌ها برای نیروهای مسلح ابزاری نوین و کارآمد هستند که می‌توانند پیشرفت‌هایی را در حوزه‌ی دفاعی پدید آورند و هم‌زمان نیز می‌توان به کمک آنها مفهوم جنگ دوپایه و شبکه‌ای را عینیت بخشید. (حبیبی، ۱۳۹۳: ۴)

در کلیه‌ی حوزه‌های ماموریتی مترتب به آن که ارتقاء توان رزم در این حوزه را در پی دارد، از اینرو نگه‌داشت و اجرای تداوم ماموریتی با لحاظ کلیه تهدیدات متبادر بر آنها بررسی وضعیت آنها و میزان آسیب‌پذیری در مقابله با انواع تهدیدات هوایی قابل شناسایی محتمل اعم از سامانه‌های کنترل و فرماندهی پهپادها، جنگنده‌های نسل چهارم و پنجم موجود در اختیار کشورهای فرامنطقه‌ای و منطقه‌ای و در ثانی وجود سپر دفاع هوایی قوی زمینی و انواع تهدیدات نظیر جنگ الکترونیک، سایبر، سایبر الکترونیک و... جملگی تهدیدات جدی در خصوص شناسایی پرنده‌های موجود با در نظر داشتن فاکتورهای مهم شناسایی آنها نظیر شکل و اندازه و ظاهر موجود درخشش آفتاب، لوله‌آگزوز موتور، نشرهای فرکانس رادیویی، نقاط داغ و تسلیحات نصب شده در زیر پرنده به صورت ملموس جهت شناسایی راداری و انواع سنجنده منصوب بر روی سامانه‌های یاد شده دشمن ( اعم از هوایی و زمینی ) محسوب می‌گردند، از اینرو صرفاً به حوزه‌ی ماموریتی پهپادهای اهداف خاص و راهبردی رزمی شناسایی پرداخته شده است

مورد شناسایی و هجمه قرار نگرقتن در برابر انواع تهدیدات هواپایه، انواع پهپادهای راهبردی و سامانه‌های پشتیبانی‌کننده آنها از سوی دشمن مرتبط با پرنده‌ها در سه بخش کلی خواهد بود:

- کاهش یا حذف قدرت شناسایی و یا مورد هدف قرار گرفتن پرنده‌ها قبل از پرواز (سامانه‌های

زمینی و پهپاد )

- کاهش یا حذف قدرت شناسایی و یا مورد هدف قرار گرفتن حین پرواز (ارتباط بین پهپادها و سامانه های کنترل زمینی)

- کاهش یا حذف قدرت شناسایی و یا مورد هدف قرار گرفتن هنگام فرود  
با توجه به قابلیت ها و توانمندی های دشمن در حوزه هوافضا و برتری نسبی آنها در این حوزه ها، بایستی به امنیت پروازی و دفاع از پهپادهای خودی در مراحل مختلف پروازی (زمان قبل پرواز، حین پرواز و هنگام فرود)، باید توجه داشت در صورت عدم انجام چنین تحقیقی، ممکن است امکان بهره مندی از پهپادها را در زمان هرگونه درگیری با هر یک از کشورهای منطقه ای و فرا منطقه ایی با کاهش توان استفاده بهینه ماموریتی مختلف را همراه سازد. از این رو به منظور استفاده حداکثری از بعد سوم نبرد با استفاده از پهپادهای راهبردی یعنی قدرت هوایی ایجاب می نماید تا با پیاده سازی راهکارهای تکمیلی نتایج این تحقیق به دنبال حداقل آسیب پذیری در مقابله با تهدیدات هوایی بوده تا افزایش سطح توانمندی پهپادها را در مقابله با انواع تهدیدات هوایی را در بر داشته باشد.

هدف اصلی این تحقیق ارتقاء توان قدرت هوایی پرنده های بدون سرنشین (پهپاد) راهبردی در برابر تهدیدات هوایی می باشد.

هدف های فرعی نیز - تبیین سطح توانمندی پرنده های بدون سرنشین (پهپاد) راهبردی قبل پرواز در مقابله با تهدیدات هوایی

تبیین سطح توانمندی پرنده های بدون سرنشین (پهپاد) راهبردی حین پرواز در مقابله با تهدیدات هوایی

تبیین سطح توانمندی پرنده های بدون سرنشین (پهپاد) راهبردی هنگام فرود در مقابله با تهدیدات هوایی می باشد.

## مبانی نظری

### الف - پیشینه شناسی:

تهدیدات هواپایه قابلیت ها و تهدیدهای نوپدیددی در عرصه نظامی و دفاعی بر علیه پهپادهای راهبردی ایجاد کرده اند. چگونگی بهره برداری یا مقابله مؤثر با این تهدیدها موضوع مطالعات و پژوهش های متعددی بوده است. برخی از پژوهش هایی که در گذشته در ارتباط با موضوع در کشور انجام شده با رویکرد تهدیدات، ارتقاء توان رزم با نگاه به آینده در جدول (۱) ارائه شده است.

جدول ۱: پژوهش‌های انجام‌شده در زمینه‌ی ارتقاء توان رزم پهپاد و تهدیدات هوایه

پژوهشگر و سال	عنوان پژوهش	نتایج
پیشینه با لحاظ ارتقاء توان رزم با نگاه به آینده		
حسن شکوهی، علی همت‌عندلیبی : تابستان ۱۳۹۱	آرایه‌های پهپادهای مطلوب در صحنه نبرد ناهمگون برای اجرای ماموریت اطلاعاتی	هواییمای بدون سرنشین از جمله تجهیزات پیشرفته عصر حاضرند که در جنگ‌های آینده جایگاه ویژه‌ای خواهند داشت. بنابراین نیازمند پهپادهای اطلاعاتی با قابلیت‌های متناسب با ماموریت‌های اطلاعاتی (شناسایی، مراقبت و هدف‌یابی، جمع‌آوری الکترونیک(شنود)) هستیم.
محمد اسدی فر : بهار ۱۳۹۴	نقش پهپادها در ایجاد امنیت و اشراف اطلاعاتی منطق مرزی کشور	با توجه به تهدیدهای مناطق مرزی کشور بخش قابل ملاحظه‌ای از توان نیروهای امنیتی و در راس آن فرماندهی مرزبانی کشور صرف مقابله با پدیده‌هایی چون شرارت، قاچاق و عبور از مرز... می‌گردد، لذا می‌تواند در کنار بکارگیری از منابع انسانی از تجهیزات جدید بهره‌گیری نمود تا علاوه بر اشرافیت اطلاعاتی فتلفات و هزینه‌ها را هم کاهش داد. بهتر است طراحی و ساخت و توسعه این گونه تجهیزات در دستور کار سیاست‌گذاران امنیتی کشور قرار گیرد.
سرهنگ مخابرات و جنگال ستاد محمد رضا باستانی : اردیبهشت ۱۳۹۰	بررسی چگونگی بکارگیری هوایماهای بدون سرنشین در انواع عملیات جنگال و ارتباطی و ارائه الگوی تاکتیکی و تکنیکی متناسب	با این میزان توانمندی و تجهیزات جنگالی نزااجا نمی‌تواند در هنگام رویارویی با نیروهای فرا منطقه‌ای مقابله کند.
هادی باغبانی: فصلنامه مطالعات دفاعی و استراتژیک، ۱۳۹۹	رأیه راهبردهای بکارگیری پهپادهای فوق پیشرفته در حوزه امنیت ملی جمهوری اسلامی ایران	نتایج تحقیق را با بیان راهبرد‌های استخراج شده مبنی بر " راهبردهای تهاجمی " با بهره‌جستن از قوتها درصدد بهره‌برداری از فرصت‌ها برآمده که در همین راستا به منظور تعیین ترتیب و توالی و اولویت بندی راهبردهای این حوزه در قالب QSPM موارد ذیل معین شد.
جیمز جانسون ( James S. Johnson ) در سال	هم‌انداز چین از میدان نبرد به محور شبکه: سایبر، فضا و چالش‌های نامتقارن	این مقاله به تقاطع پارادایم نظامی فرمان، کنترل، ارتباطات، رایانه‌ها، اطلاعاتی، نظارت و شناسایی در حال تحول، با چالش‌های نامتقارن سایبر، فضا و جنگ الکترونیک در حال تحول در

ایلات متحده در شبکه آینده محور می پردازد.	ترومغناطیسی برای ایالات متحده	۲۰۱۹
در این مقاله برابر با عنوان با یک نگاه راهبردی و توسعه ایی به بیان توسعه ایی پهپادها در راستای ارتقاء توان رزم پرداخته شده است	بردهای توسعه بهره گیری پهپاد در افزایش توان رزمی نیروهای مسلح	احمدیان، پورصادق، شریفان (نویسنده مسئول) فصلنامه مطالعات دفاعی و استراتژیک ۱۳۹۷
پیشینه با لحاظ تهدیدات		
<p>محقق در این تحقیق بر این مسئله است که ارتباط بین پرنده و ایستگاه زمینی (لینک ارتباطی) و سامانه هدایت و کنترل مبتنی بر (هدایت GPS) مورد حمله سایبری واقع نگردد و از طرفی سنجنده های الکترواپتیکی و راداری مبتنی بر امواج الکترومغناطیسی قادر به کشف و شناسایی پهپادها و ایستگاه های کنترلی نباشند. با تکمیل یافته های تحقیق، پاسخ سوالات اصلی و فرعی ارائه گردید. به طوری که:</p> <p>برای سوال فرعی یکم یعنی: پیشرانهای طرح راهبردی مصون سازی پرنده های بدون سرنشین در برابر تهدیدات سایبر الکترومغناطیس چیست؟ این پیشرانها بر اساس نظر خبرگان و جامعه نمونه در ۷ مورد قوت و ۳ مورد فرصت لیست گردید.</p> <p>برای سوال فرعی دوم یعنی: چالشهای طرح راهبردی مصون سازی پرنده های بدون سرنشین در برابر تهدیدات سایبر الکترومغناطیس چیست؟ این پیشرانها بر اساس نظر خبرگان و جامعه نمونه در ۹ مورد ضعف و ۷ مورد تهدید لیست گردید.</p> <p>با توجه به پاسخ سوالات فرعی، پاسخ سوال اصلی تحقیق یعنی: طرح راهبردی مصون سازی پرنده های بدون سرنشین در برابر تهدیدات سایبر الکترومغناطیس چیست؟ نیز حاصل شد و مطابق جدول شماره شش این راهبردها به ترتیب اولویت ذکر گردید.</p>	تدوین راهبردهای پدافند غیرعامل پرنده های بدون سرنشین در برابر تهدیدات سایبر الکترومغناطیس	هادی باغبانی: فصلنامه مطالعات دفاعی و استراتژیک ۱۴۰۱

<p>در این مقاله ضمن مرور قابلیت‌ها و ویژگی‌های فضای سایبر و الکترونیک، به هم افزایی ایجاد شده در این دو حوزه می‌پردازد. در پایان به بررسی بدافزار هوشمند به عنوان یکی از اصلی‌ترین سلاح‌های حوزه سایبر الکترونیک پرداخته و نمونه-ای از کاربردها و چالش‌های این حوزه در نیروی هوایی و سایر کاربردهای آن ارائه شده است.</p>	<p>مروری بر نبرد سایبر الکترومغناطیس و بهره برداری از سلاح‌های هوشمند سایبری</p>	<p>توسط مصطفی عباسی و مهدی دهقانی که در سال ۱۳۹۴ طی چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه</p>
---	--	--

### ب- مفهوم شناسی:

**تعریف راهبرد:** راهبرد، نوع خاصی از راه و روش دستیابی به هدف‌هایی است که شرایط سه‌گانه بلند مدت بودن، محیط رقابتی و جنبه حیاتی داشتن را دارا؛ به عبارتی راهبرد، تعیین‌کننده چگونگی دستیابی به هدف‌های بلند مدت و حیاتی سازمان است که در محیط رقابتی قرار دارد. (مردانی، ۱۳۹۵: ۱۰).

**قدرت هوایی:** توان کلی یک ملت برای پرواز و اقدام از طریق آسمان با استفاده از پرواز کنترل شده هواپیما، تعریف می‌کنند. (نصیرزاده، ۱۳۹۳، ۸۱).

- "توانایی بهره‌گیری از بعد سوم (ارتفاع) به منظور تاثیرگذاری بزرگ موقعیت و یا دشمن" در این تعریف فضا جزئی از بعد سوم و همین‌طور تمامی نیروهای نظامی و هوانوردی کشوری در مجموعه قدرت هوایی قرار می‌گیرند (نصیرزاده، ۱۳۹۳، ۸۱).

**تهدید:** دو واژه تهدید و امنیت در کنار هم می‌آیند لذا با وجود تهدید اعم از داخلی و خارجی واژه امنیت معنا پیدا می‌کند. چنان‌که "مک سوینی" اظهار داشته، بعد سخت‌افزاری یا متصلب تهدید از دیرباز مد نظر کلیه بازیگران و تحلیلگران بوده است. دلیل این امر به ویژگی‌های بارز این بعد باز می‌گردد که عبارتند از:

یک: واقعی بودن<sup>۱</sup> دو: عینی بودن<sup>۲</sup> سه: محسوس بودن<sup>۳</sup>

بر این اساس مشخص می‌شود که "تهدید" عامل عینی، محسوس و واقعی است. که منافع بازیگر را از ناحیه بیرون (ویا به شکل درونی ولی با حمایت مرزهای بیرونی) به مخاطره می‌افکند. این بعد تهدید قابل اندازه‌گیری و تعیین میزان شدت می‌باشد. (افتخاری، ۱۳۸۵: ۲۸).

<sup>1</sup> Objective

<sup>2</sup> Visible

<sup>3</sup> Tangible

**تهدید سخت:** هرگاه به موجب اقداماتی استقلال و تمامیت ارضی کشور در خطر (بالفعل یا بالقوه) هجوم نیروهای نظامی کشور دیگر یا اتحادی از کشورهای خارجی یا گروه های معارض مسلح داخلی قرار گیرد، تهدید سخت واقع شده است. در این تهدید عمدتاً، هدف اشغال سرزمین و دستگاه سیاسی کشور است. تهدیدات سخت متکی به روش های فیزیکی، عینی، سخت افزارانه و همراه با اعمال و رفتارهای خشونت آمیز، براندازی آشکار و با استفاده از شیوه زور و اجبار و حذف دفاعی و اشغال سرزمین است. (عبدالله خانی، ۱۳۸۳: ۴۵).

**پهپاد:** به هواگردی گفته می شود که فاقد سرنشین بوده و برای ایجاد نیروی برآی مورد نیاز، از نیروهای آیرودینامیکی استفاده می کند و می تواند به صورت اتوماتیک یا با بکارگیری سیستم کنترل از راه دور در طول پرواز هدایت شود. این قبیل هواگردها در دو نوع هواپیما و بالگرد طبقه بندی می شوند که با توجه به تعدد کاربردهایشان قابلیت حمل محموله های متنوعی اعم از انفجاری و غیر انفجاری را دارا می باشند و بنابر ماموریتشان در دونوع یکبار مصرف و قابل بازیافت ساخته و بکارگرفته می شوند، به طور کلی هر جا امکان بکارگیری نیروی انسانی به دلایلی وجود نداشته باشد و یا مقرون به صرفه نباشند، وسایل هدایت پذیرزمینی، دریایی و هوایی وارد عمل شده و جایگزین بخش نیروی انسانی می شوند. (ملک زاده، سادات شجاعی، ۱۳۹۰: ۴۴)

**تهدیدات هواپایه:** امکانات و مقدرات مختلف کشورهای جهان به همراه نوع تهدید در ابعاد مختلف شامل انواع هواپیماها، بمب ها، موشک ها، رادارها و تجهیزات شناسایی و جاسوسی، دقت عمل آنها، قدرت آنها و چگونگی بکارگیری و هدایت و ناوبری و نحوه ی انفجار و اثرات تخریب آنها بدست آید. (حسنی، ۱۳۸۷: ۲۳).

### تعاریف عملیاتی

**تهدیدات هواپایه:** خطراتی که سلامت پروازی پهپادها را تهدید می نماید به دو دسته کلی تقسیم می شوند دسته اول مخاطرات بیرونی و دسته دوم مخاطرات درونی می باشند در مخاطرات بیرونی احتمال کشف، شناسایی رهگیری و انهدام برخورد تصادفی با هر نوع شی پرنده و خرابکاری در سامانه های اویونیک و مکانیکی توسط عوامل نفوذی، دشمن مختل شدن به عمد و یا غیر عمد سامانه موقعیت یاب جهانی عملیات جنگ الکترونیک دشمن و یا تداخل فرکانس تصادفی وجود دارد در مبحث مخاطرات درونی نقص فنی و از کار افتادن ناگهانی قطعات اویونیک و مکانیکی و یا اپتیکی خبط و خطای کروی پرواز در هدایت و کنترل و روند اجرای مأموریت، نقص فنی در ایستگاه های هدایت و کنترل زمینی و سایر اشکالات فنی محتمل می باشد علاوه بر این تهدیدات علیه سامانه های پروازی، ایستگاه های هدایت و

کنترل زمینی نیز در معرض تهدید حملات هوایی و خرابکاری عناصر نفوذی می باشند.  
(حسن زاده ۱۴۰۱: ۲۱)

**تهدیدات حوزه کشف و شناسایی:** اطلاع دشمن از شروع پرواز پهپاد و مسیر حرکت آن با استفاده از عوامل نفوذی و شنود.

✓ ارتباطات رصد اپتیکی، طیف مادون قرمز و سیگنالی و راداری سامانه های پهپاد توسط دشمن که در منطقه مأموریت حضور دارند.

✓ استفاده دشمن از سامانه های سنجش از دور حرارتی با قابلیت چرخش خودکار در سمت و ارتفاع که تهدیدی جدی برای کشف پهپادها خواهد بود.

✓ استفاده دشمن از حسگرهای صوتی در نقاط مرتفع و یا بر روی بالن جهت رهگیری صوتی پهپادها.

✓ استفاده دشمن از تجهیزات جاسوسی جهت شنود تصویر داده ها و امواج و سیگنال های ارسالی از پهپاد.

✓ استفاده دشمن از رادارهای فرکانس بالا به منظور کشف پهپادهای پنهان کار.

✓ استفاده دشمن از رادارهای هوا پایه جهت رهگیری فعالیت های پهپادها.

✓ استفاده دشمن از رادارهای مولتی استاتیک جهت رهگیری.

✓ استفاده دشمن از رادارهای لیزری جهت رهگیری پهپادها. (حسن زاده ۱۴۰۱: ۲۱)

**تهدیدات در حوزه انهدام و مقابله:** با توجه به اینکه عمده سامانه های پهپادی ما دارای سرعت های بالایی نیستند لذا در صورت رهگیری توسط بالگردهای رزمی و هواپیماهای دشمن به راحتی سرنگون خواهند شد.

✓ سامانه های آتش در شبکه پدافند یکپارچه و چندلایه توان سرنگونی پهپادها را خواهند داشت.

✓ اختلال بلند مدت سامانه های موقعیت یاب جهانی باعث سردرگمی و سقوط پهپادها خواهد شد.

✓ ایجاد میدان الکترومغناطیس قوی در محیط پروازی و اطراف یک سامانه ی پهپادی باعث از کار افتادن سامانه های اویونیک و رایانه های سامانه پهپادی و در نتیجه سقوط آن ها خواهد شد.

✓ ایجاد خطا در سامانه های ناوبری پهپاد با ایجاد خطا در سامانه GPS.

✓ انهدام ایستگاه های هدایت و کنترل از طریق حملات هوایی یا عملیات های نفوذی و کماندویی.

✓ حملات الکترومغناطیس و سایبری به ایستگاه های هدایت و کنترل.

✓ تشکیل بانک سیگنالی از باگ های اطلاعاتی ارسالی به پهپاد و ارسال رندومی باگ های ارسالی به پهپاد خودی جهت ایجاد اختلال در پهپاد خودی.

✓ استفاده از پهپادهای هوشمند رهگیر جهت انهدام پهپاد از سوی دشمن. (حسن زاده ۱۴۰۱: ۲۳).



### جزئیات تهدیدات هواییه پهپادها

با توجه به بخش قبلی که به بیان عمده تهدیدات هواییه متبادر بر پهپادها پرداخته شد حال به منظور شناخت جامع نسبت به جزئیات تهدیدات هواییه منصوب بر پهپادها و دستیابی به مدلی از این تهدیدات، در سه سطح به واکاوی آنها پرداخته می شود، سطح اول مربوط به ابعاد آن است که به ترتیب عبارتند از: سخت، نیمه-سخت و نرم، که به ترتیب متناسب با هر بعد مولفه ها و شاخص های مربوطه نیز احصاء شده اند مراتب تشریح گردیده و در نهایت به جزئیات به تبیین موضوعات پرداخته و متناسب با هریک از ابعاد مولفه و شاخص مربوطه تشریح جامع گردیده است.

**ابعاد تهدیدات هواییه پهپادها:** در این پژوهش ما سه بعد را برای تهدیدات هواییه در نظر گرفته ایم. برای هر یک از این ابعاد مؤلفه هایی در نظر گرفته و با شاخص گذاری این مؤلفه ها، چگونگی اثرگذاری آنها بر ارتقاء قدرت هوایی را واکاوی می کنیم.

**بعد سخت تهدیدات هواییه:** تهدید سخت، عبارت از اعمال قدرت نظامی برای تحمیل اراده و تأمین منافع است. در این نوع تهدید، هدف، اشغال سرزمین است. تهدید سخت، متکی بر روش های فیزیکی، عینی و سخت افزارانه است. (عبدالله خانی، ۱۳۸۳: ۴۵)

**بعد نیمه سخت تهدیدات هواییه:** تهدید نیمه سخت عبارت از اعمال قدرت از راه نفوذ در نظام سیاسی - امنیتی یک کشور، برای تحمیل اراده و تأمین منافع است (عبدالله خانی، ۱۳۸۳: ۴۵)

**بعد نرم تهدیدات هواییه:** تهدید نرم مجموعه اقداماتی است که باعث دگرگونی هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام سیاسی شود. «تهدید نرم» نوعی سلطه در ابعاد سه گانه حکومت، اقتصاد و فرهنگ است (عبدالله خانی، ۱۳۸۳: ۴۵).

### مؤلفه های تهدیدات هواییه سخت

**هواییم:** هواییم یا طیاره نوعی هواگرد بال ثابت است که توسط موتور جت یا پیستونی به پرواز در می آید.

**بمب:** یک بمب نوعی از مهمات است که توسط هواییم با طرح قبلی در هنگام پرواز برای نابودی نفرات و تجهیزات بر روی هدف انداخته می شود. (اصلائی، ۱۳۹۱: ۴۵).

با توجه به مأموریت بمبها به صورت زیر طبقه بندی گردیده اند:

- بمب های GP
- بمب های شیمیایی
- بمب های ترکیبی
- بمب های آموزشی
- بمب های آتش زا
- بمب های الکترومغناطیسی و گرافیتی

طبقه بندی بمبها با توجه به مواد داخلی آن:

- بمب‌هایی که مواد منفجره قوی دارند.
- بمب‌هایی که مواد شیمیایی دارند مانند مواد شیمیایی دودزا -گازی آب‌زا.
- بمب‌های آتش‌بازی<sup>۱</sup>
- بمب‌هایی که جهت آموزش استفاده می‌شود. آموزشی - تمرینی.

**راکت:** اولین راکت به مفهوم امروزی توسط شاهزاده حیدرعلی در هندوستان ابداع شد که این راکت در نیمه دوم قرن ۱۷ علیه انگلیسی‌ها به کار گرفته شد. این راکت‌ها لوله‌هایی از آهن و ماده اصلی آن را باروت تشکیل می‌داد.

### مولفه های تهدیدات هوایایه نیمه سخت

**جنگ الکترونیک:** جنگ الکترونیک یا جنگال (کوتاه‌شده جنگ الکترونیک) اصطلاحی نظامی و بیانگر کاربرد الکترونیک و امواج الکترومغناطیس در نبردهاست و شامل ارتباطات رادیویی، ایجاد اختلال در ارتباطات رادیویی دشمن و شنود (استراق سمع) گفتگوهای دشمن است.

**ماهواره:** امروزه، ماهواره‌ها به بخشی مهم و عمده در زیربنای ساختار ارتباطات و اطلاعات تبدیل شده‌اند، بطوری که با اطمینان می‌توان هزاره سوم میلادی را قرن ماهواره‌ها نام گذاشت. تکنولوژی ماهواره، عاملی قوی برای تغییر و دگرگونی است. این تکنولوژی، می‌تواند چون ابزار مفیدی به انسان کمک کند تا با استفاده از آخرین پدیده‌های علمی، زندگی دلخواه و آرمانی پر بار و پرتلاش داشته باشد.

**بالن:** بالون، گونه‌ای هواگرد است که به دلیل شناوری، در جو باقی می‌ماند. بالون با نیروی باد در آسمان به حرکت درمی‌آید.

**سایبر الکترونیک:** وجود سامانه‌ها و سامانه‌های کنترلی و پردازشی موجود مخابراتی، ناوبری و سنسورهای تصویر برداری در پهپادها برای اعمال فرامین و دریافت اطلاعات محیطی آنها را در مقابل حملات سایبری و الکترونیکی (EA) آسیب پذیری نماید. این حملات می‌تواند در قالب: مختل کردن، فریب دادن، بی اثر کردن یا از بین بردن (تخریب) تسلیحات الکترونیکی، الکترونیکی، مخابراتی و راداری (تجهیزات دشمن) به منظور سلب استفاده آن از طیف الکترومغناطیسی باشد.

### تهدیدات سایبری

**فضای سایبر:** فضای سایبر به مجموعه‌ای از ارتباطات انسان‌ها از طریق رایانه‌ها و وسایل مخابراتی در یک محیط غیر فیزیکی و الکترونیکی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. که در آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود و کاربران آن می‌توانند از طریق رایانه‌ها با یکدیگر ارتباط برقرار کنند (Coonfield, 2013: 28).

<sup>۱</sup> PYROTECHNIC

**سایبرالکترومغناطیس:**

اقدامات الکترومغناطیس سایبری، فعالیت‌های موثری جهت تسخیر، حفظ و بهره‌برداری از یک برتری بیشتر در برابر مخاصمان و دشمنان در هر دو حوزه فضای سایبری و طیف الکترومغناطیسی هستند، بطوریکه استفاده مشابه و همزمان دشمن و مخالفان را کاهش می‌دهد و از مأموریت سیستم فرماندهی نیز محافظت می‌کند. این اقدامات شامل عملیات‌های فضای سایبری ۱، نبرد الکترونیکی ۲ و عملیات مدیریت طیف ۳ است (Coonfield, 2013: 28).

**✓ عملیات‌های فضای سایبری**

عملیات‌های فضای سایبری، استفاده از امکانات فضای سایبری است که هدف اصلی آن دستیابی به اهدافی است که در راستای فضای سایبری است. عملیات‌های فضای سایبری شامل سه بخش است: عملیات‌های فضای سایبری تهاجمی ۴، عملیات‌های فضای سایبری دفاعی ۵ و عملیات شبکه اطلاعات و وزارت دفاع ۶ (Bender, 2013: 4)

**بخش‌های سایبری پهپادها و سامانه‌های کنترلی زمینی:****✓ بخش‌های سایبری پهپادها**

بخش‌های مختلف سایبری عبارتند از: باتری‌ها، موتور، توزیع کننده برق، رایانه مدیریت پرواز، مودم ارسال داده، سامانه هدایت ناوبری ماهواره ایی، آنتن فرمان و انتقال داده، پردازش کننده ثبت کننده تصویر، سنسور زاویه حمله، عملگرهای فلپ، دوربین دید در شب، موشک‌های راداری و تلویزیونی

**✓ تجهیزات اویونیک لازم عبارتند از:**

- Data manager<sup>v</sup>
- INS
- رادیو رله
- ضبط کننده اطلاعات (RECORDER)
- IFF
- RADIO RELAY
- MODULAR Pressing Assembly) MPCA
- رایانه اصلی پرواز و رایانه مفید و دستورهای مخصوص
- GGS برای ناوبری

---

1 Cyber Operations (CO)

2 Electronic Warfare (EW)

3 Spectrum Management Operations (SMO)

4 Electromagnetic Spectrum (EMS)

5 Offensive Cyberspace Operations (OCO)

6 Department of Defense Information Network Operations (DODIN)

- جایرو پیزوالکتریک برای ناوبری و پایداری
- سنسورهای داده های هوایی برای اندازه گیری ارتفاع و سرعت و سنسورهای موتور
- الکترونیک مربوط به منبع تغذیه

#### ✓ ایستگاه کنترل زمینی

برای ارتباطات بین پرنده و ایستگاه زمینی می توان بعنوان مثال از باندهای رادیویی از قبیل UHF RADIO که دارای برد تا ۱۵۰ کیلومتر می باشد و یا ایستگاه های ماهواره ای استفاده نمود.

ایستگاه کنترل زمینی دارای مولفه های ذیل می باشد :

- سازمان فرماندهی عملیات ۱
- صفحه نمایش ناوبری ۲
- پایانه زمینی از راه دور ۳
- محفظه پردازش سیگنال رایانه ای ۴
- تسهیلات برنامه ریزی ماموریت ۵
- کنترل محیطی ۶
- قفسه های ارتباطی ۷
- کنسول محموله های عملیاتی

#### مولفه های تهدیدات هوای پایه نرم

✓ فضای رسانه ای فضای سایبری

#### شاخص های تهدیدات هوای پایه سخت

✓ هواپیمای شکاری (جنگنده)، هواپیمای ترابری، بالگرد، پهپاد

#### شاخص های بمب در تهدیدات هوای پایه سخت

✓ بمب گرافیتی، بمب الکترومغناطیسی، بمب لیزری

#### شاخص های موشک در تهدیدات هوا پایه سخت

✓ موشک آیرودینامیکی، موشک بالستیکی، موشک کروز

#### شاخص های راکت در تهدیدات هوا پایه سخت

✓ راکت شلیک مستقیم، راکت هدایت شونده

#### شاخص های جنگ الکترونیک در تهدیدات هوا پایه نیمه سخت

حمله الکترونیکی (آفند الکترونیکی)، فاظت الکترونیکی<sup>۱</sup>، اطلاعات الکترونیکی، پارازیت الکترونیکی، فریب الکترونیکی<sup>۲</sup>، فریب الکترونیکی جعلی، فریب الکترونیکی شبیه سازی،

<sup>1</sup> Mission Commanders Console

<sup>2</sup> Navigation Display

<sup>3</sup> Remote Ground Terminal

<sup>4</sup> Computer Signal Processing Rack

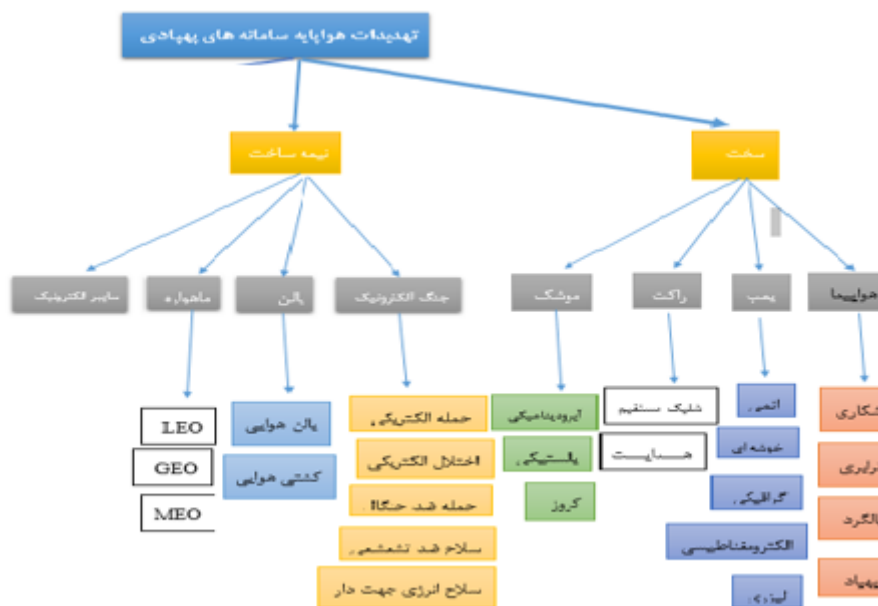
<sup>5</sup> Mission Planning Facility

<sup>6</sup> Environmental Control

<sup>7</sup> Communication Racks

فرب الکترونیکی تقلیدی، فرب تقلیدی ارتباطی<sup>۳</sup>، فرب تقلیدی غیر ارتباطی، فرب تقلید راداری، فرب ناوبری، فرب سیستم های کنترل از راه دور، فرب جعلی ارتباطی<sup>۴</sup>، اختلال الکترونیکی، پارازیت رسان

### چار چوب مفهومی



شکل ۱: تهدیدات هوایی سامانه های پهپادی

### روش شناسی

این تحقیق به لحاظ هدف کاربردی می باشد که جهت گردآوری داده ها از روش توصیفی-پیمایشی استفاده شده است. همچنین قلمروهای تحقیق، از منظر زمان بررسی سال ۱۳۹۸ و از نظر قلمرو کاربردی شدن راهبردها و قابل بهره برداری بودن نتایج آن، تا افق سند چشم انداز کشور و تا زمانی که مولفه های محیطی تغییر نکرده باشند معتبر خواهد بود و از نظر مکانی، به واسطه سطح راهبردی آن در سطح کل نیروهای مسلح و همچنین از نظر موضوع در حوزه پدافند غیرعامل در برابر تهدیدات سایبرالکترونیک می باشد. جامعه آماری مورد تحقیق ۱۲ نفر از خبرگان (ستاد کل ن.م، ودجا، سازمان پدافند غیرعامل، آجا و سپاه پاسداران) و ۵۰ نفر از مدیران میانی ستاد نهاجا (با

<sup>۱</sup> -جنگ الکترونیک برای صحنه نبرد دیجیتالی-مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، سال ۱۳۸۵

<sup>۲</sup> Electronic Deception

<sup>۳</sup> Imitative communication Deception

<sup>۴</sup> Manipulative Communication Deception

احتساب ضریب امنیتی و با استفاده از روش نمونه‌گیری تصادفی ساده می‌باشد. برای جامعه خبرگان نفراتی برگزیده شده‌اند که در حوزه پهپاد و سایبرالکترونیک صاحب‌نظر بوده و یا در این خصوص تحقیقاتی داشته‌اند. در تحلیل داده‌ها از فنون مختلف آمار استنباطی (T) تک نمونه‌ای و ماتریس ارزیابی) به کمک نرم‌افزار spss استفاده شده‌است. روایی پرسشنامه که جمع‌آوری اطلاعات تحقیق از طریق پخش آن در بین افراد جامعه نمونه (۵۰ نفر از مدیران میانی ستاد نهایج) و سپس جمع‌آوری آن به دست آمده، با بکارگیری نظرات خبرگان، مورد بررسی و تأیید قرار گرفت. به کمک محاسبه مقدار آلفای کرونباخ نیز پایایی پرسشنامه به میزان ۰/۸۱۳ بدست آمد.

جدول ۲: آمار پایایی

تعداد آیتم‌ها	ضریب آلفای کرونباخ
۴	۰/۸۱۳

### تجزیه و تحلیل داده‌ها و یافته‌های تحقیق:

بر اساس نظر خبرگان با تلاقی عوامل محیطی داخلی و خارجی مبتنی بر مولفه‌های قوت و فرصت مورد بررسی و احصا قرار گرفت. موارد به دست آمده جهت تأیید نهایی طی پرسشنامه در جامعه نمونه توزیع گردیده که نتایج تحلیل آن با استفاده از آزمون T تک نمونه‌ای به شرح جداول ذیل می‌باشد.

جدول ۳: نتیجه بررسی موارد قوت (One-Sample Test)

	مقدار آزمون=۳					
	آماره (T)	درجه آزادی (Df)	معیار تصمیم Sig. (2-tailed)	میانگین اختلافات	فاصله اطمینان ۹۵٪ اختلافات	
					کران پایین	کران بالا
Q1	۳/۸۸۰	۴۹	۰/۰۰۰	۱/۴۸۰۰۰	۰/۷۱۳۵	۲/۲۴۶۵
Q2	۳/۹۷۱	۴۹	۰/۰۰۰	۱/۵۴۰۰۰	۰/۷۶۰۷	۲/۳۱۹۳
Q3	۰/۷۷۰	۴۹	۰/۰۴۵	۰/۲۶۰۰۰	۰/۴۱۸۹	۰/۴۵۱۱
Q4	۳/۴۱۲	۴۹	۰/۰۰۱	۱/۴۴۰۰۰	۰/۵۹۱۹	۲/۵۸۷۴
Q5	۶/۳۰۷	۴۹	۰/۰۰۰	۲/۳۴۰۰۰	۱/۵۹۴۴	۳/۲۴۵۵
Q6	۵/۰۹۶	۴۹	۰/۰۰۰	۱/۷۴۰۰۰	۱/۰۵۳۹	۲/۸۶۴۵
Q7	۵/۰۹۶	۴۹	۰/۰۰۰	۱/۷۴۰۰۰	۱/۰۵۳۹	۲/۱۶۲۲

جدول ۴: نتیجه بررسی موارد فرصت (One-Sample Test)

مقدار آزمون=۳	

	آماره (T)	درجه آزادی (Df)	معیار تصمیم Sig. (2-tailed)	میانگین اختلافات	فاصله اطمینان ۹۵٪ اختلافات	
					کران بالا	کران پایین
Q1	۴/۴۸۵	۴۹	۰/۰۰۰	۱/۵۵۰۰۰	۰/۷۴۱۳	۲/۲۴۶۵
Q2	۲/۸۷۸	۴۹	۰/۰۰۰	۱/۳۶۰۰۰	۰/۲۳۲۳	۲/۳۱۹۳
Q3	۱/۸۷۵	۴۹	۰/۰۳۵	۰/۷۴۰۰۰	-۰/۷۴۴۴	۰/۹۳۸۹

با توجه به اینکه در جداول One-Sample Test مقدار  $\text{Sig. (2-tailed)} < ۰/۰۵$  این بدان معناست که میانگین امتیاز موارد بررسی شده برابر ۳ نمی‌باشد. از سوی دیگر با توجه به اینکه مقدار آمار میانگین اختلافات مثبت می‌باشد در نتیجه میانگین امتیاز مولفه مورد نظر بیش از ۳ بوده و این مولفه مورد تأیید قرار می‌گیرد. با توجه به نتایج فوق قوت‌ها و فرصت‌ها عبارتند از:

#### لیست قوت‌ها:

۱. وجود مراکز علمی و تحقیقاتی نظامی که در حوزه طراحی، تولید و ساخت پهپادها فعالیت دارند.
۲. برخورداری از کارکنان دارای تحصیلات عالی به میزان ۶۰ درصد از کل کارکنان نیروهای مسلح.
۳. برخورداری از کارکنان متعهد و متخصص در سطح سازمان‌های نظامی و غیر نظامی.
۴. بهره‌مندی از اختیارات و حمایت‌های قانونی.
۵. بهره‌مندی از اعتبارات تحقیقاتی مورد نیاز.
۶. توان بالای علمی، فن‌آوری و تحقیقاتی کشور در حوزه علوم مخابرات، الکترونیک و دیتا.
۷. وجود ارتباط مناسب و قابلیت توسعه آن با مراکز علمی، پژوهشی و آموزشی و امکان استفاده از تمام ظرفیت‌های تولیدی و توسعه دانش پدافند غیرعامل در این حوزه.
۸. وجود بستر لازم صنعت نانو مواد در خصوص ساخت و بهره‌گیری مواد جاذب راداری در طراحی پهپادهای با سطح پایین مقطع راداری (قابلیت رادارگریزی).
۹. امکان نصب لینک ارتباطی امن، قابل نصب بر روی پهپادها جهت برقراری ارتباط با ایستگاه کنترلی زمینی.

#### لیست فرصت‌ها:

۱. امکان استفاده از ظرفیت‌ها و امکانات ارتباط و مخابراتی در سطح نیروهای مسلح.
۲. امکان هم‌پیمانی و اشتراک منافع با همسایگان و کشورهای منطقه و فرامنطقه‌ای.

۳. امکان کسب فن‌آوری و دانش از محیط بین‌المللی.

بر اساس نظر خبرگان، دو قسمت ضعف‌ها و تهدیدات مورد بررسی و احصا قرار گرفت. موارد به دست آمده جهت تأیید نهایی طی پرسشنامه در جامعه نمونه توزیع گردیده که نتایج تحلیل آن با استفاده از آزمون T تک نمونه‌ای به شرح جداول ذیل می‌باشد:

جدول ۵: نتیجه بررسی موارد ضعفها (One-Sample Test)

مقدار آزمون=۳						
	آماره (T)	درجه آزادی (Df)	معیار تصمیم Sig. (2-tailed)	میانگین اختلافات	فاصله اطمینان ۹۵٪ اختلافات	
					کران پایین	کران بالا
Q1	۳/۵۴۶۴	۴۹	۰/۰۰۰	۱/۵۸۰۰۰	۰/۹۸۹۲	۲/۶۵۲۵
Q2	۳/۴۱	۴۹	۰/۰۰۰	۱/۵۴۰۰۰	۰/۵۸۳۵	۲/۳۱۶۳
Q3	۰/۶۸۵۶	۴۹	۰/۰۴۵	۰/۱۱۰۰۰	-۰/۵۵۸۲	۰/۷۴۴۱
Q4	۳/۵۴۶۵	۴۹	۰/۰۰۱	۱/۴۰۰۰۰	۰/۵۲۳۳	۲/۸۵۱۲
Q5	۶/۲۴۱۵	۴۹	۰/۰۰۰	۲/۰۴۰۰۰	۱/۳۹۶۱	۳/۹۱۰۰
Q6	۵/۴۲۵۲	۴۹	۰/۰۰۰	۱/۹۶۸۰۰	۱/۰۴۵۸	۲/۰۲۵۴
Q7	۵/۰۱۳۲	۴۹	۰/۰۰۰	۱/۹۸۸۸۰	۱/۸۵۷۵	۲/۳۲۱۰
Q8	۰/۷۸۰	۴۹	۰/۰۲۵	۰/۲۸۵۰۰	۰/۴۰۰۹	۰/۴۵۸۱
Q9	۳/۹۰۲	۴۹	۰/۰۰۱	۱/۴۴۳۰۰	۰/۵۶۴۹	۲/۵۰۰۴

جدول ۶: نتیجه بررسی موارد تهدیدات (One-Sample Test)

مقدار آزمون=۳						
	آماره (T)	درجه آزادی (Df)	معیار تصمیم Sig. (2-tailed)	میانگین اختلافات	فاصله اطمینان ۹۵٪ اختلافات	
					کران پایین	کران بالا
Q1	۳/۷۴۱	۴۹	۰/۰۰۰	۱/۵۰۰۰۰	۰/۹۶۸۲	۳/۶۵۲۵
Q2	۳/۴۱۱۰	۴۹	۰/۰۰۰	۱/۱۱۱۰۰	-۰/۴۱۶۲	۱/۸۵۴
Q3	۰/۴۷۱۱	۴۹	۰/۰۰۰	۰/۰۳۵۰۰	۰/۱۰۲۱	۱/۴۱۵۱



مقدار آزمون=۳						
	آماره (T)	درجه آزادی (Df)	معیار تصمیم Sig. (2-tailed)	میانگین اختلافات	فاصله اطمینان ۹۵٪ اختلافات	
					کران بالا	کران پایین
Q4	۳/۶۲۳	۴۹	۰/۰۰۱	۱/۷۴۴۰۰	۰/۵۰۶۳	۱/۷۴۹۶
Q5	۱/۰۲۱۱	۴۹	۰/۰۰۰	۲/۳۹۹۰۰	۱/۰۱۷۴	۳/۹۸۷۴
Q6	۵/۰۰۲۱	۴۹	۰/۰۰۰	۱/۷۰۱۰۰	۱/۸۵۴۱	۲/۳۶۵۲
Q7	۳/۰۵۴۶	۴۹	۰/۰۰۱	۱/۸۷۸۷۰	۰/۱۲۱۱	۲/۷۴۸۷

با توجه به اینکه در جداول One-Sample Test مقدار  $0/05 < \text{Sig. (2-tailed)}$  این بدان معناست که میانگین امتیاز موارد بررسی شده برابر ۳ نمی‌باشد. از سوی دیگر با توجه به اینکه مقدار آمار میانگین اختلافات مثبت می‌باشد در نتیجه میانگین امتیاز مولفه مورد نظر بیش از ۳ بوده و این مولفه مورد تأیید قرار می‌گیرد. با توجه به نتایج فوق ضعف‌ها و تهدیدات عبارتند از:

#### لیست ضعف‌ها:

لیست ضعف‌ها در دفتر فصلنامه موجود می‌باشد.

#### لیست تهدیدات:

۱. تنوع و گستردگی تجهیزاتی کشورهای منطقه‌ای و فرمانطقه‌ای (اعم از با سرنشین و بدون سرنشین).
۲. در اختیار بودن سامانه هدایت و کنترل GPS (سامانه موقعیت‌یاب جهانی) در اختیار دشمن.
۳. دارا بودن سنجنده‌های قوی الکترواپتیکی در کشف و شناسایی پهپادها و سامانه‌های کنترلی.
۴. دارا بودن سنجنده‌های قوی راداری در کشف و شناسایی پهپادها در هنگام پرواز.
۵. شناخت مناسب دشمن از ضعف‌ها و آسیب‌پذیری‌های عملکردی پهپادها و سامانه‌های مربوطه.
۶. امکان حمله به پهپادها به روش سایبرالکترونیک.
۷. عدم امکان خرید خارج انواع محصولات بدلیل افزایش گسترده تحریم.
۸. داشتن قدرت هوافضایی در زمینه کشف، شناسایی و انهدام در کلیه مراحل قبل، حین و هنگام فرود پهپادهای راهبردی
۹. دارا بودن تسلیحات (انواع موشک و بمب های هوایی) دور ایستای هدایت ماهواره‌ای

**ارائه راهبرد:**

در این تحقیق هر راهبرد بر اساس دو ویژگی ذیل تدوین گردیده است:  
الف: چالش‌ها را برطرف نماید (چالش‌ها بر گرفته از نقاط ضعف و تهدید).  
ب: از پیشران‌ها استفاده شود (مبتنی بر نقاط قوت و فرصت).

از اینرو باتوجه به تجزیه و تحلیل راهبردی مبتنی بر چهار عامل یاد شده راهبردهای پدافند غیرعامل تحقیق در برابر تهدیدات سایبرالکترونیک برای رسیدن به وضع مطلوب تدوین گردیده است. راهبردها با استفاده از عوامل پیشران‌ها (قوت‌ها و فرصت‌ها) به منظور رفع ضعف‌ها و پاسخ به تهدیدات به روش نخبگی تدوین گردیدند که در نهایت تعداد ۱۱ راهبرد ارائه و پاسخ به سئولات فرعی حاصل شد. سپس پرسشنامه ارزیابی راهبردها تهیه و بین نخبگان جهت مقایسه و انطباق راهبردها با هریک از عوامل چهارگانه محیطی توزیع گردید که با استفاده از پاسخ‌های جمع‌آوری شده و همچنین وزن برای هریک از عوامل محیطی، ماتریس ارزیابی راهبردها جهت محاسبه میزان مطلوبیت هر راهبرد صورت پذیرفت. بعلاوه با توجه به اینکه به دلیل محدودیت در تامین منابع و... امکان اجرای تمامی راهبردها وجود ندارد، لذا ضروری است نسبت به اولویت‌بندی راهبردها و قرار گرفتن راهبردهای دارای اولویت بالاتر، در راس برنامه‌های اجرایی اقدام شود. بنابراین میزان مطلوبیت راهبردها با استفاده از تکنیک "تعیین رجحان ترتیبی به وسیله شباهت به جواب ایده‌آل" محاسبه گردید که جهت این امر، بر اساس ماتریس ارزیابی راهبردها و انجام مراحل شش گانه محاسباتی تکنیک مذکور، مطلوبیت‌های هریک از راهبردها به دست آمد.

در مرحله بعد، جهت اولویت‌بندی راهبردها به این روش اقدام گردید: راهبرد با بالاترین مقدار مطلوبیت، به عنوان بالاترین اولویت برای اجرا تعیین گردید و بر همین اساس، اولویت‌بندی راهبردها براساس بالاترین میزان، مطلوبیت و به ترتیب نزولی از مقدار مطلوبیت بیشتر به مقدار مطلوبیت کمتر انجام پذیرفت.

جدول ۷: ماتریس ارزیابی و اولویت‌بندی راهبردها

مقدار مطلوبیت	دفع تهدیدات	بکارگیری فرصتها	ارتقاء قوتها	رفع ضعفها	
-	۰/۲۷۹۰	۰/۲۰۹۳	۰/۲۳۲۵	۰/۲۷۹۰	وزن عوامل محیطی
۰/۹۷۹۷	۴/۶	۴/۳	۴/۷۵	۴/۱۶	راهبرد ۱
۰/۶۷۷۲	۴/۶۵۴۵	۴/۳۵	۴/۴۵	۳/۱۸۶۶	راهبرد ۲

۰/۶۴۴۷	۴/۲۵۴۵	۴	۴/۰۵	۳/۴	راهبرد ۳
۰/۶۱۹۹	۴/۴	۴	۴/۰۵	۳/۲۴	راهبرد ۴
۰/۶۰۵۰	۴/۴	۴/۲	۳/۸	۳/۲۴	راهبرد ۵
۰/۵۷۳۷	۳/۸	۳/۲۷۵	۳/۹۵	۳/۶۸	راهبرد ۶
۰/۵۴۲۰	۴/۲۷۲۷	۳/۳	۴/۴۵	۳/۰۴	راهبرد ۷
۰/۵۲۹۷	۳/۲	۳/۸۷۵	۴/۱	۳/۶	راهبرد ۸
۰/۵۱۲۳	۴/۴	۳/۴۷۵	۳/۴۵	۳/۲	راهبرد ۹
۰/۴۳۰۸	۳/۶	۳/۲	۳/۸۵	۳/۲۴	راهبرد ۱۰
۰/۴۲۷۲	۳/۶	۳/۸	۳/۹۵	۳	راهبرد ۱۱
۰/۳۹۷۳	۳/۸	۳/۰۲۵	۴/۰۵	۲/۹۲	راهبرد ۱۲

جدول ۸: لیست راهبردها بر اساس اولویت آنها

تاثیر بر تحقق اهداف کلان پدافند غیرعامل کشور					راهبرد	ردیف
تسهیل مدیریت بحران	ارتقاء پایداری ملی	تداوم فعالیت های ضروری	افزایش بازدارندگی	کاهش آسیب پذیری		
		*	*	*	مصون سازی، استحکام بخشی و امن سازی لینک ارتباطی امن و پایدار بین پرنده های بدون سرنشین و ایستگاه های کنترلی.	۱
	*	*			طراحی و پیاده سازی سامانه هدایت و کنترل پرنده های بدون سرنشین	۲
				*	طراحی و پیاده سازی نظام دفاعی در برابر تهدیدات سایبری الکترونیک جهت ایستگاه کنترلی زمینی و پهپادها	۳
	*			*	طراحی و ساخت پرنده های بدون سرنشین با قابلیت پنهان سازی امن، مصون، مستحکم در برابر تهدیدات شناسایی راداری دشمن.	۴
				*	بستر سازی مناسب به منظور بهره مندی حداکثری از تمام پتانسیل علمی کشور اعم از مراکز علمی وابسته به مراکز نظامی و غیر نظامی و مراکز دانش بنیان.	۵

کشور	تاثیر بر تحقق اهداف کلان پدافند غیرعامل					راهبرد	ردیف
	تسهیل مدیریت بحران	ارتقاء پایداری ملی	تداوم فعالیت های ضروری	افزایش بازدارندگی	کاهش آسیب پذیری		
*	*	*	*	*	*	طراحی و ساخت سامانه های زمینی بومی و امن اعم از کنترلی و پرتابگر به صورت تجمع شده (با حداقل سامانه، تجمع سامانه کنترلی و پرتابگر به منظور هدایت و کنترل پرنده ای با ماموریت برد متوسط و بلند) با قابلیت مصون سازی در مقابله با تهدیدات شناسایی الکترواپتیکی از سوی سکوهای هوایی و از طرفی تهدیدات الکترونیک.	۶
*	*	*	*	*	*	تدوین استانداردهای لازم بومی امنیت و دفاع سایبری، سامانه های کنترلی منصوب بر پهپادها با استفاده از مراکز علمی و تحقیقاتی و فنی موجود	۷
*	*	*	*	*	*	توسعه و روز آمدی علمی، تخصصی، آموزش نیروی انسانی با استفاده از پتانسیل های آموزشی، علمی، تخصصی موجود به منظور ارتقاء دانش تخصصی متخصصان و مسئولان در شناخت تهدیدات الکترومغاطیس سایبری	۸
*	*	*	*	*	*	برنامه ریزی به منظور سنجش سطح آمادگی مصادیق اصول موضوع تحقیق چابک سازی، بازیابی و بازسازی تجهیزاتی، کارآمدی، پاسخگویی در برابر تهدیدات حوزه سایبر الکترونیک.	۹
*	*	*	*	*	*	طراحی و ساخت سامانه های بومی و امن	۱۰
*	*	*	*	*	*	ایجاد بستر مناسب ایستگاه کنترل زمینی دینی	۱۱
*	*	*	*	*	*	مصون سازی سامانه های کنترلی زمینی با شل دینگ مناسب در برابر به منظور کاهش آسیب پذیری در برابر انواع تهدیدات الکترونیک.	۱۲

## نتیجه گیری:

از آنجاکه شاکله اصلی و رکن مهم بعد سوم جنگ قدرت هوایی بوده و بخشی از آن بهره‌مندی از پرنده‌های بدون سرنشین با انواع قابلیت‌های مأموریت به عنوان سرمایه ملی محسوب می‌گردند، بررسی وضعیت آنها و میزان آسیب‌پذیری در مقابله با انواع تهدیدات سایبرالکترونیک مهم است. لذا به طور کلی دغدغه محقق در این تحقیق بر این مسئله است که ارتباط بین پرنده و ایستگاه زمینی (لینک ارتباطی) و سامانه هدایت و کنترل مبتنی بر (هدایت GPS) مورد حمله حملات سایبری واقع نگردد و از طرفی سنجنده‌های الکترواپتیکی و راداری مبتنی بر امواج الکترونیکی قادر به کشف و شناسایی پهپادها و ایستگاه‌های کنترلی نباشند.

تحلیل داده‌ها توسط روشهای T تک نمونه‌ای و ماتریس ارزیابی به کمک نرم‌افزار spss صورت گرفت. پایائی پرسشنامه با محاسبه مقدار آلفای کرونباخ به میزان  $0/813$  بدست آمد. با توجه به جداول آزمون T تک نمونه‌ای، مقدار  $0/05 < \text{Sig. (2-tailed)}$  و مثبت بودن مقدار آمار میانگین اختلافات مولفه‌های "قوت‌ها و فرصت‌ها" و "ضعف‌ها و تهدیدات" مورد تأیید قرار گرفتند.

## پیشنهادها:

۱. در خصوص راهکارهای عملی مصون‌سازی، استحکام‌بخشی و امن‌سازی، لینک ارتباطی امن و پایدار بین پرنده‌های بدون سرنشین و ایستگاه‌های کنترلی تحقیق و پژوهش انجام گیرد.
۲. برنامه ریزی اجرایی و اولویت بندی نتایج مستخرجه راهبردهای منظور شده در جدول ارائه راهبردها "جدول شماره ۶" (قبل از پرواز، حین پرواز، هنگام فرود) منطبق با تجزیه و تحلیل آماری
۳. نظام جامع دفاعی در برابر تهدیدات سایبری الکترونیک جهت ایستگاه کنترلی زمینی و پهپادها طراحی و پیاده‌سازی شود.
۴. با همکاری سازمانهای دانش‌بنیان و مراکز علمی و تحقیقاتی، در خصوص تدوین استانداردهای لازم بومی امنیت و دفاع سایبری و همچنین طراحی و ساخت سامانه‌های زمینی بومی و امن و پرنده‌های بدون سرنشین با قابلیت پنهان‌سازی امن، مصون، مستحکم در برابر تهدیدات شناسایی اپتیکی و راداری دشمن اقدام لازم صورت پذیرد.
۵. راه کارهای اجرایی در خصوص بهره‌گیری از ایستگاه‌های کنترل زمینی دفنی

## فهرست منابع

### الف - منابع فارسی:

- افتخاری، اصغر. (۱۳۸۵). کالبد شکافی تهدید. تهران: انتشارات سپاه.
- افتخاری، اصغر. (۱۳۹۵). مراحل بنیادین اندیشه در مطالعات امنیت ملی. تهران: انتشارات پژوهشکده مطالعات راهبردی (چاپ دوم).
- اصلانی، یعقوب (۱۳۹۳) سلاح استراتژیک جهان، تهران، سازمان عقیدتی سیاسی ارتش جمهوری اسلامی ایران
- باغبانی، هادی. (۱۳۹۳). ملاحظات پدافند غیرعامل در مقابله با تسلیحات غیرکشنده (بمب‌های الکترونیکی و گرافیتی). تهران: دانشکده علوم و فنون فارابی.
- باغبانی، هادی. (۱۴۰۱). مصون سازی زیرساخت های حیاتی در مقابله با تهدیدات الکترومغناطیسی. تهران: دانشگاه علوم و فنون هوایی شهید ستاری.
- باغبانی، هادی. (۱۴۰۱). رابطه تهدید با امنیت ملی و مدیریت بحران. تهران: مرکز مطالعات، تحقیقات و تدوین آیین نامه های رزمی پدافند هوایی آجا.
- باغبانی، هادی. (۱۳۹۸). راهبردهای بکارگیری پهپادهای پیشرفته در حوزه امنیت ملی. تهران: فصلنامه مطالعات دفاعی و استراتژیک، دانشکده دفاع، دانشگاه و پژوهشگاه عالی دفاع ملی.
- باغبانی، هادی. (۱۳۹۹). تدوین راهبردهای پدافند غیرعامل پرنده ای بدون سرنشین در برابر تهدیدات الکترومغناطیس. تهران، فصلنامه مطالعات دفاعی و استراتژیک، دانشکده دفاع، دانشگاه و پژوهشگاه عالی دفاع ملی.
- باغبانی هادی (۱۴۰۱)، الزامات طرح راهبردی مصون سازی پایگاه های هوایی جمهوری اسلامی ایران در برابر تهدیدات الکترومغناطیسی، تهران، فصلنامه مطالعات دفاعی و استراتژیک، دانشکده دفاع، دانشگاه و پژوهشگاه عالی دفاع ملی.
- پیوند، حمید (۱۴۰۱)، آسیب پذیری ستاد نهجا در مقابل با تهدیدات ریز پرنده ها، دانشکده علوم و فنون فارابی
- حبیبی، نیک بخش (۱۳۹۳)، پهپاد در عملیات هوایی، مرکز انتشارات راهبردی نهجا.
- جلالی فراهانی غلامرضا، ۱۳۹۱، انواع تهدیدات و نحوه بررسی و ارزیابی آنها، سازمان پدافند غیر عامل کشور، چاپ اول.
- جلالی فراهانی غلامرضا، هاشمی فشارکی سیدجواد، ۱۳۸۹، دفاع (پدافند) غیر عامل در آیینة قوانین و مقرارت، سازمان پدافند غیر عامل کشور، تهران.
- حبیبی نیک بخش، ۱۳۹۳، پهپاد در عملیات هوایی، مرکز انتشارات راهبردی نهجا.
- حبیبی نیک بخش، آینده پژوهشی و دفاعی سال دوم شماره ۴ بهار ۱۳۹۶
- حبیبی نیک بخش، ارائه مدل اثربخش بکارگیری بهینه پهپاد در توانمندسازی عملیات آینده
- حسن زاده، محمد رسول (۱۴۰۱)، بررسی چگونگی افزایش سطح توانمندی پرنده های بدون سرنشین (پهپاد) در مقابله با تهدیدات هوایی در راستای ارتقاء قدرت هوایی، تهران، دانشکده علوم و فنون هوایی شهید ستاری
- خرازیان محمدی، ۱۳۹۷، جنگال در جنگ های آینده، انتشارات دافوس آجا
- خرم فعال حسین، ۱۳۹۹، تهدیدات ریز پرنده ها و راه های مقابله با آن، انتشارات معاونت آموزش و پژوهش ستاد کل نیروهای مسلح، مرکز راهبردی آیین نامه های ن.م.
- دانایی محمد مهدی، ۱۳۹۰، بررسی تهدیدات الکترو مغناطیسی و سناریو های تهدید، دانشگاه آزاد اسلامی واحد الکترونیکی، چاپ دوم.

- دانایی محمد مهدی، رضایی رکن آبادی محمود، علیدوستی علی، حاجی آبادی محمد ابراهیم، خان محمد مهدی، ۱۳۹۲، تحلیل احتمالی اثر حفاظت الکترو مغناطیس بر قطعی سرویس دهی و هزینه نگهداری مراکز داده، دانشگاه جامع امام حسین (ع)، دانشکده و پژوهشکده مهندسی فناوری اطلاعات و ارتباطات، هفتمین کنفرانس علمی فرماندهی و کنترل ایران، ۱۹ و ۲۰ آذر ماه ۱۳۹۲.
- درپنهانها، علی، ۱۳۹۴، جمع آوری اطلاعات ارتباطی، انتشارات چاپخانه دانشگاه پدافند هوایی خاتم الانبیا (ص).
- رزم خواه محمد رضا، ۱۳۹۰، نقش حساسه های جمع آوری اطلاعات در دفاع غیر عامل، بوستان حمید، چاپ اول.
- رسولی غلامرضا، عادل حسن، ۱۳۹۱، تسلیحات مبتنی بر امواج الکترو مغناطیسی، سازمان چاپ و انتشار ایران جام، چاپ اول
- عباسی، مصطفی و مهدی دهقانی، ۱۳۹۴، مروری بر نبرد سایبر الکترونیک و بهره برداری از سلاح های هوشمند سایبری، چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه، تهران، دانشگاه افسری و تربیت پاسداری امام حسین، دانشکده علوم و مهندسی دفاعی
- عبدالله خانی علی، ۱۳۸۶، تهدیدات امنیت ملی (شناخت و روش)، انتشارات موسسه فرهنگی مطالعات و کتابت بین المللی ابرار معاصر تهران، تهران.
- فراتر میکائیل، رایان میکائیل (Michael R. Frater, Michael Ryan)، ۱۳۸۵، جنگ الکترونیک برای صحنه های نبرد دیجیتال، مترجمین (عقیقی احمد، کریم زاده مرثی، نظافتی محمد باقر)، موسسه آموزشی کتابت صنایع دفاعی، طرح فراسازمانی فاوا نیروهای مسلح، چاپ دوم.
- قاسم آبادی داود و حسن نعمتی، ۱۳۹۸، معرفی ریزپرنده ها (MAVS) و ارائه روش کشف و شناسایی آنها، پنجمین همایش ملی علوم و مهندسی دفاعی، تهران، دانشکده علوم و مهندسی دفاعی دانشگاه افسری و تربیت پاسداری امام حسین (ع).
- گودرزی علی، ۱۳۹۷، اطلاعات سیگنالی، انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- مرادی یونس، ۱۰، ۱۳۹۷، روش شکار پهپاد؛ از لیزر مرگبار تا هک در آسمان، <https://digiato.com>.
- میر سمیعی محمد، ۱۳۹۰، دانستنی های پدافند غیر عامل (ویژه دوره عالی رشته ای کارشناسان و کارمندان همتراز)، انتشارات دانشگاه هوایی شهید ستاری، چاپ اول.
- نوروزی احمد، ۱۳۹۴، بررسی حملات الکترونیکی علیه پهپادها، چهارمین همایش ساسری علوم و مهندسی دفاعی در سپاه، ۱۱ اسفند ۱۳۹۴.
- نیازی مجید، ۱۳۸۸، آشنایی با پرنده های بدون سرنشین هدایت پذیر، سازمان صنایع هوایی نیروهای مسلح.
- یازی، مجیدرضا، (۱۳۸۸)، آشنایی با پرنده های بدون سرنشین هدایت پذیر از راه دور / ارون، تهران، سازمان صنایع هوایی ن.م. (شرکت صنایع هوایی قدس).
- والتز ادوارد (Edward Waltz)، ۱۳۸۶، جنگ اطلاعات اصول و عملیات، مترجمین (رنجبر اکبر، حاج قاسم حسن، فخرایی محمود)، موسسه آموزشی کتابت صنایع دفاعی، طرح فراسازمانی فاوا نیروهای مسلح، چاپ دوم.

### منابع انگلیسی:

- Applications of high power micro waves, salisbury, dstoerl, Ewd. 1993.draft paper.
- Army, U.S. "Army Doctrine Publication (ADP) No.3-0,2011, Unified land Operations". Headquarters Department of the Army Washington, DC,10 October.
- Army.U.S. "Field Manual No,3-13, (2013): Inform and Influence Activities". Headquarters Department of the Army Washington, DC,25 January.

- Barbara OpalRome, "Israel Makes for Broad Space Capabilities, Space News.com
- Website, Augst 25,2003.
- Bar-Lev, Schering, Leonid, Vola Levin, EROS System-Satellite orbit and constellation design,
- 22nd Asian Conference on Remote Sensing-Singapore, 2001.
- Bender, J.M, & Hamilton, A. (2013) The Cyberspace Operations Planner. Jornal Article/ Nov,5(11),18am.
- B. H. P. Maathuis, and J. L. Van Genderen, "A review of satellite and airborne sensors for remote
- Sensing based detection of minefields and landmines," International Journal of Remote Sensing,
- Vol. 25 No.23, pp. 5201-5245, 2004.
- Bodson D., Electromagnetic Pulse &the Radio Amateur"Parte 1, Acting Assistant Manager, Tecnology&Standards National Communication System, Washington, DC20305-2010, August 1986.
- Caris, Michael & et al,2017, Detection and tracking of micro aerial Vehicle with millimeter wave radar, European Radar Conference(EuRAD).
- CCRS: Canada Centre of Remote Sensing, Educational Resources for Radar Remote Sensing
- Field Manual (FM) 3-38, (2014), Cyber Electeromagnetic Activities, Headquarters, Department of the Army Washington.
- FM 20-3, US Army-Camouflage, CalmestndDeception, pp.29. 1994.
- Introduction to RADAR Remote Sensing, 2006.
- Kopp C., "The Electromagnetic Bomb-a Weapon of Electrical Mass Destruction", DefenceAnalyste, Melbourne, Australia,

#### سایت‌ها:

- URL-1. <http://www.iai.co.il>
- URL-2. <http://www.house.gov/hasc>
- URL-3. <http://www.ostp.gov/NSTC/html/pdd8.htm>
- URL-4. <http://www.users.ox.ac.uk/~daveh/Space/Military>
- URL-5. <http://rst.gsfc.nasa.gov/Front/tofc.html>, Military Intelligence Satellites, 2007.
- URL-6. [www.fas.org/spp/military/afwa/metsat-u3.htm](http://www.fas.org/spp/military/afwa/metsat-u3.htm)
- URL-7. Satellites, and UAVs, Official Rules and Modeling System for the Global