

دفاع غیر عامل و تهاجمات الکترونیکی

کمیته پژوهش‌های راهبردی معاونت پژوهش و تولید علم^۱

چکیده

در این مقاله، محقق درصدد آن است که مشخص نماید چگونه می‌توان با استفاده از امکانات کشور قدرات عامل و غیر عامل سامانه جنگ‌های الکترونیکی را برای مقابله با تهدیدات احتمالی دشمن ارتقا داد؛ به طوری که آمادگی رزمی آنان افزایش یابد؟ برای این منظور، عوامل اثرگذار بر سامانه جنگ‌های الکترونیکی به طور اعم و اخص، مورد شناسایی، بررسی و مطالعه قرار می‌گیرند. شناخت دقیق عوامل کلیدی داخلی (نقاط قوت و ضعف) و خارجی (فرصت‌ها و تهدیدات) جنگ‌ال آجا با مدنظر قرار دادن مأموریت و تاثیر آن بر توان رزمی، موجب تعیین و معرفی راهبردهای بهینه از مجموعه راهبردهای مبنای (ژنریک یا عمومی، شامل حال و آینده) شناخته شده در مجامع علمی - تحقیقی داخلی و خارجی می‌شود.

این مقاله با استفاده از روش تحقیق موردی و زمینه‌ای معرفی و تکنیک فرآیند تحلیلی سلسله مراتبی (A.H.P) از مجموعه تکنیک‌های تصمیم‌گیری چندمعیاره صورت گرفته و با ارزیابی زوجی عوامل و راهبردهای قابل اجرا و نیز اولویت‌بندی راهبردهای اجرایی از آن نتایج راهبردی خود را معرفی کرده است.

کلیدواژه:

دفاع غیرعامل، جنگ الکترونیک، جنگ اطلاعات، فریب الکترونیکی، راهبردهای عامل و غیرعامل^۲

^۱ - این مقاله حاصل تلاش‌های مطالعاتی و تحقیقاتی در کمیته راهبردی دانشگاه عالی دفاع ملی

مصوب و به پایان رسیده است

علی ستاری خواه استادیار و عضو هیات علمی دانشگاه شهید ستاری.

مقدمه

باگذشت زمان، فناوری الکترونیکی، و ارتباطی نقش بسزایی در عملیات نظامی به عهده داشته و مراحل مختلفی را پشت سر نهاده است. تاریخ الکترونیک و نخستین مرحله در معرفی تجهیزات الکترونیکی به زمان اختراع رادیو و استفاده از آن به منظور جهت یابی و شناسایی موقعیت دشمن برمی گردد.

مرحله دوم با معرفی رادار برای کشف هدف و موقعیت آن از نظر سمت و فاصله به تدریج دقت آتشبارها فزونی می یابد که آخرین مرحله و شاید مرگبارترین آن را می توان از زمان استفاده از وسایل الکترونیکی جهت هدایت دقیق موشک ها ذکر نمود.

جنگ های به وقوع پیوسته در دهه پایانی قرن بیستم در دو منطقه بحران خیز جهان (خلیج فارس و بالکان)، چشم انداز جنگ های الکترونیکی را در زمینه های معماری، طراحی و به کارگیری گسترده سامانه ها و حساسه های هوشمند، جنگ اطلاعاتی، شبکه های عصبی، تلفیق و ترکیب اطلاعات، سامانه های اطلاعاتی نوین، فناوری های پنهانکار (دور از دید سامانه های راداری)، رادارهای چند ایستایی، دام ها، کاهش احتمال ره گیری و به کارگیری رادارهای باند فوق العاده گسترده))، حساسه های مادون قرمز و الکترواپتیک، ((تجهیزاتی هدایت شونده حامل انرژی)) و ... در سامانه های فرماندهی و کنترل نیروهای مسلح کشورهای جهان در حال و آینده نشان می دهد. (جواهری، ۱۳۷۹، ۶-۱۶-۱۸)

بیان مسأله و اهمیت تحقیق

رعایت اصول جنگ، انجام به موقع و دقیق اقدامات پشتیبانی الکترونیکی، آفند یا تهاجم الکترونیکی و پدافند الکترونیکی، عملیات های تعیین کننده دیگری هستند که تضمین کننده ی تحمیل جنگ بر طرف مقابل در جنگ های پیش گفته شناخته شده است.

به همین دلیل امروزه فناوری نوین جنگ الکترونیکی نه تنها در صحنه های عملیاتی جنگ، سهم بزرگی دارد، بلکه به عنوان بعد چهارم جنگ شناخته شده است، بلکه خود به عنوان جنگ افزار پدافندی در شرایط صلح و جنگ، نوع دیگری از جنگ محسوب می گردد. (افشاری، ۱۳۶۹، ۹)

بدون تردید کشورهایی توان مقابله و ایستادگی در برابر تهاجم دشمنان خود دارند که دارای سیاست ها و راهبرد های مناسب تدوین شده از قبل، در همه ی ابعاد قدرت ملی (سیاسی، اقتصادی، اجتماعی - فرهنگی و نظامی و ...) است و قابلیت های اجرایی لازم با بهره گیری از تفکر دفاع غیر عامل در زمینه های مختلف (تخصصی)، در برابر این نوع تهاجمات را در خود جا داده باشند.

درچنین شرایطی علاوه بر راه کارهای تکنیکی و سیاسی، رسالت بخش های مسؤول و فنی بیش از پیش سنگین تر می شود و راهبرد دفاعی-امنیتی و به تبع آن راهبرد جنگ های اطلاعاتی و الکترونیکی از اهمیت و اولویت بیشتری برخوردار می گردد.

حال پرسش آغازین تحقیق براساس برخورد موقعیتی مسأله به شرح زیر مطرح می شود:

اگر زمانی کشوری مورد هجوم نظامی کشورهای قدرتمند همسایه، منطقه و فرمانطقه ای دارای جنگ افزارها، تجهیزات و سامانه های پیشرفته با امکانات و مقدرات نوین جنگ الکترونیکی قرار گیرد، مردم و نیروهای مسلح چگونه باید دفاع نمایند تا ضمن حفظ وضع موجود، با اقتدار کامل بر نیروهای خودی فرماندهی و کنترل مفید و مؤثر نماید و با انجام عملیات مناسب جنگ الکترونیکی به عنوان بخشی از اقدامات پدافند هوایی غیرعامل، سایر اقدامات پدافند هوایی عامل را پشتیبانی کند و میزان آسیب پذیری های خود را کاهش دهد و امور مدیریت بحران و جنگ را با موفقیت اعمال و اراده خود را بر دشمن تحمیل کند و کنترل حوزه ی امواج الکترومغناطیسی نیروهای مسلح خودی را به دست گیرند.

اهداف کلی تحقیق

-تدوین راهبرد بهینه دفاع الکترونیکی در زمان صلح و جنگ به منظور ارتقای توان رزمی و آمادگی رزمی نیروهای نیروهای مسلح و حراست از منابع حیاتی، حساس و مهم کشور جهت حفظ صلح پایدار و مقابله با تهدیدات الکترونیکی دشمنان بالقوه و بالفعل ج.ا.ا در زمان صلح و جنگ.

-شناخت و تدوین راهبردهای و رویکرد واقعی و قابل اجرا درزمینه‌ی ساختارهای سازمانی، نیروی انسانی، تجهیزاتی، نظام آموزشی، طبقه بندی مشاغل نیروهای مسلح، مرتبط با سامانه‌ی پدافند غیرعامل الکترونیکی.

سؤال تحقیق

-راهبرد مناسب پدافند الکترونیکی سامانه‌ی پدافند غیرعامل به منظور پشتیبانی عملیات رزمی و تقویت توان رزمی و آمادگی رزمی نیروهای مسلح در مقابله با کشورهای تهدید کننده ج.ا. چیست؟

روش تحقیق

چون پژوهش انجام شده در زمینه‌ی خاص یعنی اقدامات جنگ الکترونیکی است، بنابراین بخشی از حوزه پدافند غیرعامل محسوب، بنابراین، روش تحقیق "موردی و زمینه‌ای"^۱ است.

جامعه‌ی آماری

دراین تحقیق جامعه‌ی آماری، کارشناسان، متخصصان و خبرگان تخصصی گروه رسته‌های عملیات هوایی، پدافند هوایی، جنگ الکترونیک و جنگ اطلاعاتی که از سامانه‌های هشدار دهنده، جمع‌آوری اطلاعات (E.S.M)، تهاجم الکترونیکی (E.C.M) و دفاع الکترونیکی (E.C.C.M) در اجرای ماموریت‌های محوله استفاده می‌کنند و مدیریت نگهداری و تعمیرات تجهیزات جنگ الکترونیکی حوزه‌های مختلف هوایی، زمینی و دریایی را برعهده دارند می‌باشند.

حجم نمونه

در این پژوهش تعداد ۳۰ نفر از صاحب نظران و متخصصان امور جنگ الکترونیکی نیروهای مسلح به صورت روش نمونه‌گیری تصادفی ساده انتخاب شده و پرسشنامه‌ی تخصصی در بین آنان توزیع گردیده که پس از توجیه حضوری و تکمیل آنها؛ جمع‌آوری و مورد تجزیه و تحلیل قرار گرفته است.

^۱ Case study

محیط پژوهش

محیط های کاری دفاع الکترونیکی در یگان های عملیاتی-رزمی و پشتیبانی نیروهای مسلح و نیز واحدهای مرتبط با جنگ الکترونیکی در حوزه ی پدافند غیرعامل به عنوان محیط پژوهش می باشند.

روش گردآوری اطلاعات

باتوجه به این که نوع تحقیق کاربردی و روش اجرای آن، "موردی و زمینه ای" می باشد، روش گردآوری اطلاعات، مبتنی بر مطالعات میدانی، کتابخانه ای، مصاحبه ای، مشاهدات عینی است.

پژوهشگر با انجام مطالعه و بررسی موضوع تحقیق و بادر نظر داشتن طرح نظری مسأله تحقیق، مدل تحلیلی مناسبی ارائه داده است که در ادامه ی پژوهش با بهره گیری از یافته ها و نتایج تحقیق، اقدام به تدوین راهبرد مناسب می نماید، به نحوی که با امکانات موجود کشور، در عمل قابل اجرا باشد؛ یعنی تحقق "آن چه که باید باشد" امکان پذیر شود.

منابع و ابزار گردآوری اطلاعات

مراکز اطلاع رسانی (شبکه اینترنت، کتابخانه)، مجلات معتبر خارجی و داخلی (تخصصی)، بخش های عملیاتی، تحقیقاتی و مدیریت های دفاع الکترونیکی و جنگ اطلاعات در سطح نیروهای مسلح به عنوان منابع اطلاعات که از طریق استفاده از پرسشنامه، فیش برداری، مصاحبه با صاحب نظران و متخصصان جنگ های الکترونیکی و انجام بازدید از محیط های تحقیقاتی، صنعتی و آموزشی مرتبط با سامانه های دفاع الکترونیکی، جهت دستیابی به اطلاعات مفید مورد نیاز موضوع رساله، به عنوان ابزارهای گردآوری اطلاعات، استفاده شده است.

روش تجزیه و تحلیل اطلاعات

در تجزیه و تحلیل اطلاعات، یک بعد کمی وجود دارد که آن محاسبات آماری و اولویت و ترتیب بندی داده ها صورت می گیرد و یک بعد کیفی، که در آن تحلیل های کیفی بر اساس تعامل اطلاعات، برداشت های استنباطی و آگاهی های شهودی، با استفاده از جدول ترجیحات قضاوتی به صورت کمی نمایش داده می شود که بر اساس نتایج آماری به جامعه ی آماری مرتبط، قابل تعمیم است. در این تحقیق از هر دو بعد

ذکر شده، برای تجزیه و تحلیل اطلاعات بعد از ساختن مدل، بیان فرضیه، شناسایی متغیرهای مستقل و وابسته و تعریف عملیاتی و کمی نمودن آن‌ها استفاده شده است.

تعریف مفاهیم و اصطلاحات تحقیق

جنگ اطلاعاتی: به تهاجم همه جانبه بر روی تمامی امکانات و مقدرات اطلاعاتی دشمن (اقتصادی، سیاسی، اجتماعی-فرهنگی و نظامی و ...) به منظور فرسایش نظامی و شخصی دشمن اطلاق می‌گردد.

شبکه‌های عصبی: بر مبنای اصول کارکرد آنتن‌های آرایه‌ای فازی که از مولفه‌های متعددی برای جهت یابی در نظر گرفته می‌شوند، کار می‌کنند.

مقدرات شبکه‌های عصبی و کاربرد آن در جنگ الکترونیک:

۱- توانایی استفاده از اطلاعات مبهم.

۲- امکان گسترش شبکه‌های عصبی در حوزه‌ی اطلاعات سیگنالی یا SIGINT^۱ و افزایش کارایی

۳- افزایش سرعت و دقت در تجزیه و تحلیل سیگنال‌ها، ره‌گیری پارامترهای راداری و رادیویی، تلفیق و ترکیب اطلاعات و افزایش ضریب دقت اقدامات الکترونیکی

سامانه اطلاعاتی: سامانه‌ی جنگ الکترونیک به بهره‌گیری از سامانه‌ی اطلاعات، شبکه‌های عصبی و تلفیق اطلاعات را با یکدیگر ترکیب نموده تا بتواند یک مرکز کنترل با قابلیت اطلاعاتی و سازگاری فوق‌العاده بالا، به دست آورد.

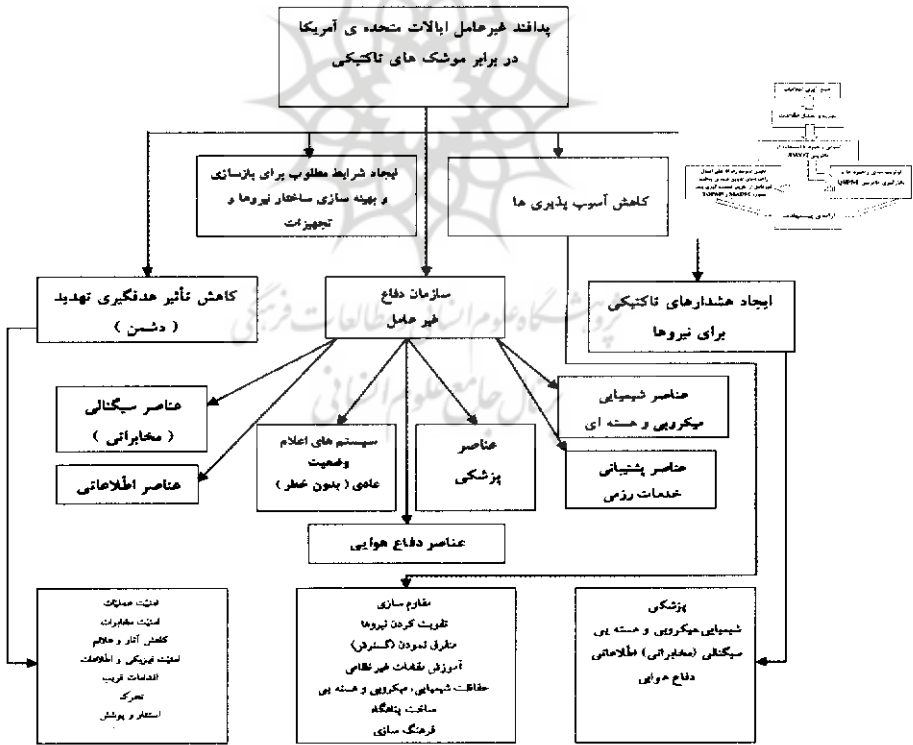
ادبیات تحقیق

ظهور جنگ اطلاعاتی در قالب جنگ الکترونیکی، جنگ شبکه‌ای و جنگ هوشمند و کاربرد آن در دکترین نظامی برای همیشه شکل و نحوه راهبری جنگ را تعیین می‌کند؛ به همین منظور کل نظام اطلاعاتی پشتیبانی کننده از یک فرمانده، هدف اصلی جنگ اطلاعاتی به شمار می‌رود و جنگ‌های الکترونیکی که زیر مجموعه‌ای از جنگ اطلاعاتی است، از دهه ۱۹۸۰ میلادی، کشورهای بلوک غرب سرگرم ایجاد تحول ((مفهومی)) به نام ((فرماندهی، کنترل، ارتباطات،

^۱ Signal intelligence

محدودیت در تعداد و ظرفیت در اکثر نقاط به آسانی قابل استفاده نبودند و ورود و خروج از آنها زمان بر و مستلزم تحمل دشواری ها و مشقاتی بود که اغلب منجر به عدم استفاده از آنها می شد.

سامانه پدافندی غیرعامل نیروهای مسلح نشان داد که در برابر حملات ددمنشانه صدام در شهرهای استفاده از شیمیایی و بیولوژیکی (میکروبی) دارای ضعف می باشد. پناهگاه های موجود فی نفسه از شرایط مناسبی به منظور حفاظت در برابر حملات شیمیایی برخوردار نبودند و همچنین ادوات و تجهیزات مناسبی نیز جهت خنثی سازی و یا پاکسازی به موقع و سریع محل های مورد تهاجم در دسترس نبودند. لازم به یادآوری است که وضعیت یاد شده ی فوق با در نظر گرفتن قابلیت و توانایی بمب ها و موشک های استفاده شده توسط رژیم بعث بیان شده است که همگی آنها از مهمات معمولی محسوب می شوند.



شکل ۱ فرآیند و مدل مفهومی انجام تحقیق

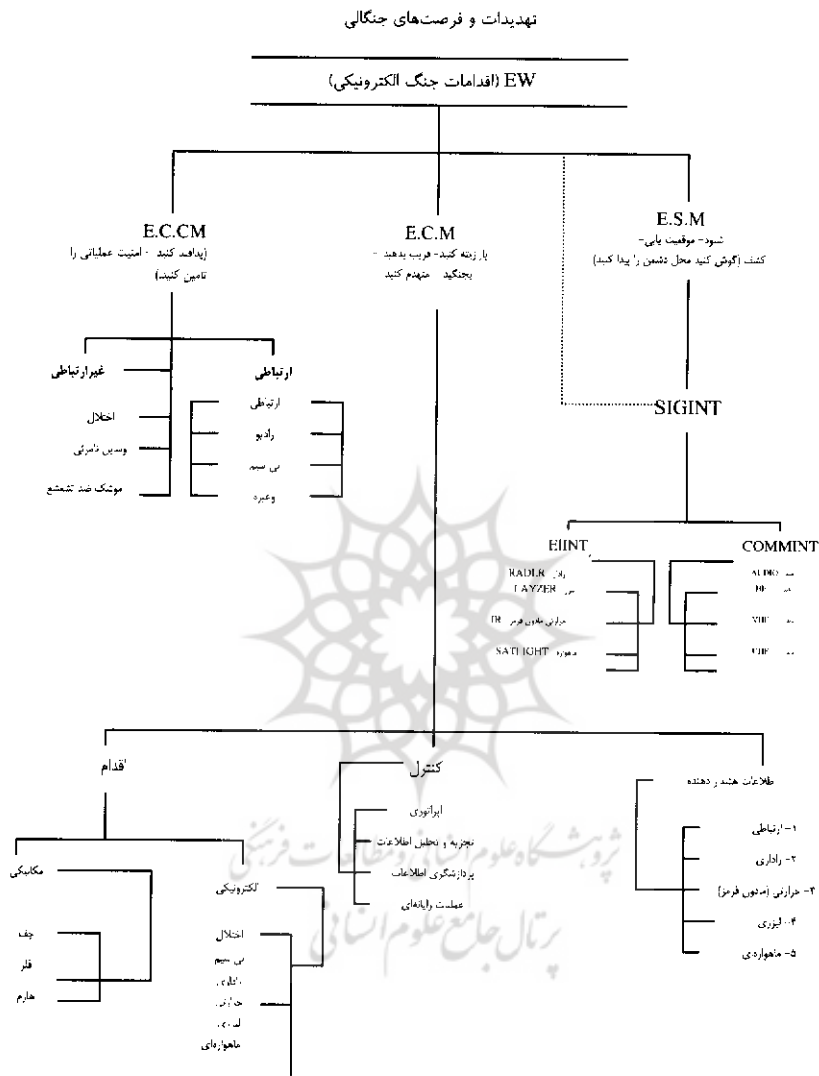
به منظور دستیابی به اهداف از پیش تعیین شده، از طریق انجام ماموریت‌های محوله به نیروهای مسلح هر کشوری، سامانه‌های جنگ الکترونیکی که در انواع تجهیزات و جنگ‌افزارهای سازمانی نیروهای مسلح (هوایی، زمینی و دریایی) به کار گرفته می‌شوند، خود دارای جداول سازمانی، تجهیزاتی و عملیاتی به شرح صفحات بعد می‌باشند و انجام موفقیت آمیز اقدامات مشروحه زیر را با در اختیار داشتن حساسه‌ها و تکنیک‌های نوین و به هنگام، نیروی انسانی آموزش دیده و سامانه‌ی فرماندهی و کنترل مناسب، میسر خواهد شد:

داشتن اطلاعات راهبردی از وسایل الکترونیکی دشمن.

۱. تحقیق و توسعه
۲. ترتیب رزمی الکترونیکی دشمن
۳. توانایی‌ها و نقاط قوت و ضعف دشمن



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی



شکل ۱ ساختار عملیاتی جنگ الکترونیک

کشف- شناسایی- ره گیری- درگیری- فریب- تخریب و انهدام

سامانه‌های دفاع الکترونیکی و اهداف عملیاتی آنها:

سامانه‌های اساسی دفاع الکترونیکی بر مبنای اهمیت و کاربرد آنها در جدول سازمانی تعیین می‌گردند. یادآوری می‌شود که اهداف عملیاتی سامانه‌های یاد شده در یک مجموعه‌ی دفاع الکترونیکی در نیروهای مسلح در قالب مجموعه‌ای از تجهیزات زیر قابل تحقق می‌باشد:

اطلاعات سیگنالی:

ماموریت سامانه‌های اطلاعات سیگنالی یا SIGINT، کسب هرچه بیشتر اطلاعات در خصوص انتشار امواج الکترومغناطیسی دشمن است. این سامانه‌ها می‌توانند به دو دسته سامانه‌های اطلاعات الکترونیکی و سامانه‌های اطلاعات ارتباطی تقسیم شوند.

اطلاعات الکترونیکی:

- تجهیزات اطلاعات الکترونیکی یا ELINT^۱ می‌باید قادر به تعیین موقعیت انتشارات الکترونیکی دشمن، مشخصات و زمان مربوطه باشند.
- توانایی تحلیل سیگنال‌های دشمن از نظر زمان، فرکانس و تعیین رابطه این سیگنال‌ها با فهرستی از تجهیزات دشمن را داشته باشند و در نتیجه این امکان را برای خود فراهم سازند که تحرکات نظامی و تجهیزات و جنگ افزارهای دشمن را در هر شرایطی تحت نظر کامل داشته باشند.

۲- اطلاعاتی ارتباطی

سامانه‌های اطلاعات ارتباطی یا COMINT^۲ مشابه سامانه‌های اطلاعات الکترونیکی ELINT می‌باشند، لیکن ماموریت آنها ره‌گیری و تجزیه و تحلیل تشعشعات ارتباطی دور و شناسایی شبکه‌های ارتباطی مربوطه است. اطلاعات ارتباطی، از طریق جمع‌آوری و تفکیک سیگنال‌های ارتباطی دشمن به دست می‌آید. (سماجا-۱۳۸۲-۱۴)

اقدامات پشتیبانی الکترونیکی (E.S.M)

^۱ Electronic intelligence

^۲ Communication intelligence

این گونه تجهیزات، با پیچیدگی متوسط تا زیاد دسته بندی می گردند. ماموریت E.S.M دریافت و ساخت مجدد یک سناریو الکترومغناطیسی، تعریف و ایجاد تهدیدهای فرضی بر اساس تهدیدهای واقعی کشورهای هدف، به منظور تمرین نیروهای خودی جهت مقابله با آنها در زمان واقعی است. این سناریو که می تواند بسیار پیچیده و ناشناخته باشد، از لحظه ره گیری توده‌ی عظیمی از سیگنال ها که به آنتن این تجهیزات وارد شده، شروع می شود.

ارتباطات - اقدامات پشتیبانی الکترونیکی

هدف این گونه سامانه‌های این است که کلیه‌ی ارتباطات دشمن را هم برای تعیین موقعیت فرستنده‌ها و سامانه‌های تقویت کننده امواج رادیویی و هم برای کشف و رمزگشایی پیام‌ها، رهگیری نماید.

اقدامات ضد الکترونیکی (E.C.M):

در یک دفاع الکترونیکی، اصولاً بهترین راه حل برای جلوگیری از شناسائی توسط دشمن، پرهیز از کشف شدن جنگ‌افزارهای آفندی است. از آنجا که سیگنال دریافتی توسط رادار، مستقیماً متناسب با سطح مقطع راداری سکو ست، کاهش موثر قدرت سیگنال راداری تولید شده توسط سکوی حفاظت شده بسیار مطلوب است (کاهش R.C.S). برای این منظور، در سال‌های اخیر فناوری جدیدی جهت مطالعه بر روی مواد و هندسه‌های ساختاری، توسعه یافته است که قادرند R.C.S هدف را به حداقل برسانند. این تکنیک‌ها معمولاً «تکنیک‌های پنهان کاری و یا پشت پرده» نامیده می شوند که خود اقدامی ضد الکترونیکی است.

پارازیت رسان‌های موج مزاحم:

این نوع پارازیت رسان‌ها، عیناً سیگنال‌هایی مطابق با فرکانس رادار دشمن تولید می کنند. این سیگنال‌ها اختلالی برابر با یک پارازیت حرارتی بسیار قوی درگیرنده‌های راداری دشمن تولید می کنند؛ بنابراین سیگنال تولید شده توسط سکو (هوآپیما، شناور و ...) به عنوان موج مزاحم، مانع رویت هدف در نمایشگرهای رادار دشمن می شود. پس هدف از پارازیت رسان موج مزاحم پوشاندن هدف‌ها توسط انتشارات سیگنال‌ها است که اختلالاتی روی صفحه نمایش رادار ایجاد می کند.

پارازیت رسان‌های فریب

سامانه‌های پارازیت رسان فریب، هدف‌های راداری کاذب تولید می‌کنند. در مورد رادارهای تجسسی (مراقبتی) این پارازیت‌ها مانع از شناسایی سکوی حقیقی (هوپیما، شناور و ...) می‌شود و در مورد رادارهای تعقیب کننده (ردیاب)، مطمئن می‌سازد که در مرحله درگیری، سامانه‌ی جنگ افزارهای موشکی، موشک خود را به طرف هدف کاذب شلیک می‌کند؛ بنابراین هدف از سامانه‌های پارازیت رسان فریب در انواع تجهیزات و جنگ افزارهای هوایی، دریایی و زمینی، محافظت از سکوی (هوپیما، شناور سطحی و زیر سطحی، جنگ افزارهای زمینی پایه) توسط فریب رادارهای دشمن با هدف‌های غیر واقعی می‌باشد.

اقدامات ضد الکترونیکی ارتباطی

هدف این سامانه‌ها، ایجاد سیگنال‌های مزاحم یا تداخل است تا این که گیرنده‌های ارتباط از راه دور دشمن را پارازیت‌ه نماید و در نتیجه پیام‌ها را غیر قابل فهم سازند. برای هرنیروی مسلحی عدم اطمینان از سامانه‌های ارتباطی خود یک مشکل عمده محسوب می‌شود.

اقدامات ضد الکترونیکی لیزری

این سامانه‌ها به منظور جلوگیری از مسافت‌یابی دقیق توسط یک سامانه‌ی جستجوگر لیزری طراحی می‌شوند و اصول کار آنها یا مشابه پارازیت‌رسان‌هایی است که در بالا ذکر شد یا ابرهایی از دود که قابلیت دید را کاهش می‌دهند، در هوا پخش می‌کنند.

اقدامات ضد الکترونیکی

تجهیزات سخت افزاری و نرم افزاری ضد الکترونیکی معمولاً به صورت بسته‌های خاص در انواع تجهیزات و جنگ افزارهای نیروهای مسلح (پدافندی، اطلاعاتی و ...) نصب و راه‌اندازی می‌شوند تا آنها را قادر سازند که در محیط الکترونیکی دشمن، یعنی در حضور پارازیت رسان‌های عمدی، علی‌رغم به حداقل رسیدن توان رزمی، همچنان پایداری لازم را از خود نشان داده و در برابر تهاجم الکترونیکی دشمن ماندگاری داشته باشند.

اقدامات ضد الکترونیکی رادارهای تجسسی

رادارهای تجسسی را می‌توان به عنوان بخش مهمی از حساسه‌های جمع‌آوری اطلاعات الکترونیکی در منطقه‌ی تحت مسؤولیت به حساب آورد که در شبکه‌ی پدافند هوایی نقش زیادی را بر عهده دارند. این نوع رادارها به انواع تکنیک‌های پدافند الکترونیکی مجهز می‌شوند تا براساس نوع تهدیدات تهاجم الکترونیکی، با تشخیص به موقع کارشناسان عملیاتی (افسران خلبان، پدافند هوایی و ...)، از تکنیک‌های یاد شده به منظور اجرای اقدامات تاکتیکی، جهت کاهش میزان اختلالات الکترونیکی هواپیماهای مهاجم دشمن، بهره‌برداری می‌کنند. با انتخاب مسیر پروازی خاص و با استفاده از دستورالعمل‌ها از همه تکنیک‌های تهاجم الکترونیکی (ECM) به جهت جلوگیری از کشف شدن در رادارهای تجسسی (مراقبتی) دشمن، اجتناب نماید.^۱

تکنیک‌ها و فناوری‌های نوین دفاع الکترونیکی

امروزه روند توسعه‌ی تکنیک‌ها و فناوری‌های جنگ الکترونیکی با شتابی بیش از هر زمان همچنان رو به تکامل است. ظهور روش‌ها و تکنیک‌های جدید، با بهره‌گیری از تجهیزات و فناوری‌های نوین، پرقدرت‌تر و حساس‌تر در حوزه‌ی امواج الکترومغناطیسی، آسیب‌پذیری‌ها را در بین کشورها در ابعاد گوناگون افزایش داده است.

تکنیک‌ها و فناوری‌های جنگ الکترونیکی جدید:

تکنیک‌ها و فناوری‌های نوین جنگ الکترونیکی موجود در نیروهای مسلح کشورهای پیشرفته و یا مورد انتظار در آینده نزدیک به شرح زیرند:

پردازش سیگنال

دسته‌بندی و ارزیابی امواج الکترومغناطیسی (ارتباطی و الکترونیکی) دشمن با سرعت، دقت و صحت فوق‌العاده زیاد، در حداقل زمان ممکن، به منظور تعیین اهمیت نظامی آرایش تجهیزات و جنگ افزارهای (هواپایه، زمین پایه، دریایاچه) دشمن در مناطق مورد نظر تعیین یا انجام اقدامات پدافند الکترونیکی، در شرایط

^۱ فیلیپوئری، مترجمین: سید محسن ساییسی و مهبد غفاری، سامانه‌های دفاع الکترونیکی ۱۳۷۹

بحران و جنگ به منظور تخمین میزان تلفات و ضایعات از جمله‌ی فناوری‌های نوین جنگ الکترونیکی در بخش «اقدامات پشتیبانی الکترونیکی» محسوب می‌گردد.

هوش مصنوعی و سامانه‌های هوشمند:

اغلب در عملیات جنگ‌های الکترونیکی، تصمیم‌گیری در وضعیتی بسیار پیچیده ضروری است.

یک سامانه‌ی جامع که قادر است هر نوع استدلال را انجام دهد، ماشینی است که دارای ویژگی‌های هوش مصنوعی باشد.^۱

سامانه‌های هوشمند، کاربرد موثری در سامانه‌های جنگ الکترونیکی نظیر E.S.M و E.C.M دارند. در حقیقت سامانه‌ی هوشمند برنامه‌ای است که می‌تواند بر روی رایانه‌های مناسب اجرا شود و مسایل مربوط به یک موقعیت معین را با استفاده از قواعد بدست آمده از دانش و تجربه هوشمند حل نماید.

آنتن‌های آرایه‌ی فازی عامل

این نوع آنتن‌ها با اجزای فراوان در حوزه‌ی جنگ الکترونیکی و راداری به منظور رفع مشکل ولتاژ بالا و طول عمر محدود TWTها، کاربرد پیدا کرده‌اند و رشد فناوری‌های آن‌ها نیز در حال افزایش است.

سطح فعلی فناوری‌های جنگ الکترونیکی و چشم‌اندازهای آن:

به نظر می‌رسد سامانه‌های E.S.M قادرند سناریوهای الکترومغناطیسی را به طور صحیح تفسیر کنند؛ با این پیش فرض که این سناریوها خیلی پر حجم و پیچیده نباشند.

اطلاعات به عنوان «سرمایه راهبردی» است و تنها موضوع کسب اطلاعات درباره جبهه با حملات تاکتیکی با شبکه‌های راداری یا تلفنی شبکه نیروی مقابل محدود نمی‌شود؛ بلکه اهرم نیرومندی مورد نظر است که بتواند مهمترین تصمیمات دشمن را دگرگون سازد؛ در حقیقت جنگ دانسته‌ها مطرح است. سخن این است که، هرطرف خواهد کوشید با دستکاری در روند دریافت و ارسال اخبار و اطلاعات، بر اقدامات دشمن اثر گذارد.

^۱ Janes defence weekly ۲۰ september ۲۰۰۰.

یک شاخص در مورد افزایش سهم عنصر دانش در جنگ، رایانه‌ای شدن آن است. امروزه جنگ از همه جنبه‌ها واقعاً خودکار می‌شود و نتیجه‌ی آن توانمندی است که مقادیر زیادی از داده‌ها را در اشکال گوناگون منتقل می‌کند. (اداره سوم سماجا، مدیریت جنگال، نشریه فرهنگ اصطلاحات جنگ الکترونیک).

بررسی تاریخی و تجربی تحقیق

گزارش پنتاگون به گنگره در زمینه راهبری جنگ خلیج فارس خاطر نشان می‌سازد «نخستین یورش ها»، برج‌های تقویت امواج کوتاه، مراکز تلفن، اتاق‌های فرمان، شبکه فیبر نوری، پل‌های حامل کابل‌های مخابراتی عراق را هدف قرارداد. هدف از این عملیات از کاراندازی سامانه‌های ارتباطی آنان و وادار کردن نیروهای عراقی در استفاده از سامانه‌های تقویتی خود بود که در برابر شنود، بسیار آسیب پذیر بودند و این اقدام اطلاعات بارزشی به دست می‌داد.

این پند را همه کشورهای در حال توسعه باید جدی بگیرند؛

امروزه، یک هواپیمای اف-۱۱۷، با یک پرواز و فروانداختن یک بمب، می‌تواند کاری را که بمب افکن‌های نیم قرن قبل با ۴۵۰۰ پرواز و انداختن ۹۰۰۰ بمب در جنگ دوم جهانی، یا با ۹۵ پرواز و ۱۹۰ بمب افکن در جنگ ویتنام می‌کردند، انجام دهد.

آن چه این کارها را می‌کند، تجهیزاتی است که به جای شاخصه حجم قدرت آتش، مبتنی بر اطلاعات است. این اطلاعات وزن مواد منفجره‌ای را که باید حمل کند، بسیار کاهش می‌دهد.

دسترسی به ارتباطات امن، دیده بانی شبکه مدار و ناوبری فضایی که بخشی از سازوکارهای مهم توانایی نظامی است با انقلابی جهانی روبروست. در آینده هر کشور خواهد توانست، جریان اطلاعات را از کم و بیش ده‌ها گیرنده دیده‌بانی، از انواع مختلف و با کیفیت گوناگون از جمله: روسی، فرانسوی، ژاپنی، حتی احتمالاً از خود آمریکا را که همه تجاری است در مقابل پرداخت پول مشترک شود.

امروزه سامانه‌ی موقعیت یاب روسی تصاویری را از راه دیده بانی به صورت تجاری با امکان تفکیک عناصر تا حد تقریبی پنج متر در دسترس قرار می‌دهد. در حالی که برای هدف‌گیری دقیق به تفکیک عناصر در حد یک متر نیاز است؛ بنابراین

هر دولتی در هر جای جهان، ممکن است به زودی بتواند چشم‌هایی در آسمان بخرد تا تصاویر واضح‌تر از محل استقرار تانک‌ها یا نفرات یا موشک‌های کشورهای دیگر با دقتی در حد ۴/۵ متر فراهم آورد.

بخش اصلاحات آتی در فناوری ناوبری به زودی می‌تواند دقت اطلاعات ماهواره‌ای آمریکا را در بالاترین درجه دقت ارائه دهند.

کمپانی موتورولا، با ارسال ماهواره‌ایی به نام ایریدیوم به صورت کمربندی گرداگرد کره خاکی، در هر جایی می‌تواند ارتباطاتی را برای استفاده کنندگان تأمین کند که اساساً در برابر پارازیت مصونیت دارد؛ به علاوه با گسترش شبکه‌های الکترونیکی در روی زمین، به زودی محروم کردن دشمن در آینده از دسترسی به اطلاعات ماهواره‌ای، ناممکن خواهد بود.

اطلاعات حساس میدان نبرد می‌تواند به سوی ایستگاه‌های تجاری زمینی و پایگاه‌های اطلاعاتی در شهرهای دنیا روانه و از طریق شبکه‌های واسط، برای ارتش‌های افغانستان، عراق فرستاده شود، این اطلاعات را می‌توان از جمله برای نشانه‌رویی و راهبری موشک‌ها به کار گرفت.

خود موشک‌های قدیمی نیز در معرض تغییرند. توانایی تغییر فناوری، موشک نسبتاً قدیمی اسکاد را به هدف‌گیری دقیق مجهز ساخت، می‌توان با تجهیز آن به یک گیرنده‌ی ناوبری تجاری با صرف هزینه‌ای حدود ۵ هزار دلار، یک اسکاد با هوش ساخت.

نقش و کاربرد جنگ‌های الکترونیکی در راهبرد دفاعی کشور

اگر راهبرد دفاعی کشور عنصر اساسی تأمین امنیت ملی است، استفاده از تجهیزات و وسایل الکترونیکی مدرن و پیشرفته از اجزای ضروری و حیاتی آن محسوب می‌گردند.

یک نیروی دریایی، هوایی و زمینی پیشرفته برای اعمال فرماندهی و کنترل فناوریانه بر یگان‌های تحت امر خود به طور فزاینده‌ای به وسایل و حساسه‌های نوین الکترونیکی متکی می‌باشد.

بر هیچ متخصص و اهل فن پوشیده نیست که جنگ الکترونیک دانشی است که به طور فعال در تحول و نوآوری است و بنا به ضرورت این حوزه به تهدیدات

فناوری‌ها که دائماً در حال تغییر و دگرگونی می‌باشند باید پاسخ دهد و این دانش، مطالعه و بررسی وسیع و خاص خود را طلب می‌کند.

وسایل و تجهیزات الکترونیکی برای برقراری ارتباطات، هدایت موشک‌ها، سامانه‌های کنترل آتش و مراقبت، رادارهای تویخانه‌ای یگان‌های شناور، وسایل کمک ناوبری و دیگر مقاصد هوایی، دریایی و زمینی به کار برده می‌شود.

نظر به این که اتکا به وسایل الکترونیکی، یک نیروی هوایی، دریایی و زمینی خواهان اقتدار و سیادت فضایی، دریایی و زمینی را در مقابل اقداماتی که دشمن به منظور کاهش کارایی این وسایل انجام می‌دهد، آسیب پذیر می‌سازد، لذا اقدامات جنگ الکترونیکی در هدایت جنگ‌ها، عامل بسیار مهم و با ارزشی شده است.

فواید جنگ الکترونیک واضح و آشکار است. برای اغلب ایستگاه‌های دریایی و یگان‌های شناور، پروازی، پدافندی و ایستگاه‌های زمینی راداری و شنود دفاع الکترونیکی وسیله‌ای جهت افزایش قابلیت بقای هدفی منفرد یا کل نیروهای درگیر می‌باشد.

در عین حال این مسأله هم وجود دارد که در زمان صلح، هنگامی که تمرینات دفاع الکترونیکی انجام می‌شود، دشمن هوشیار گردد و بتواند خود را از نظر اقدامات ضدضد الکترونیکی آماده سازد. به هر حال باید این نکته را به یاد داشته باشیم که نشان دادن این که یک طرف برای جنگیدن آماده است، مطمئن‌ترین راه جلوگیری از جنگ می‌باشد.

به عبارت ساده‌تر تصمیم گیرندگان و تدوین کنندگان راهبرد دفاعی کشور بیش از هر چیز به بازدارندگی تأکید دارند. به نظر آنان باید قدرت کشور در برابر تهدیدات مشخص کنونی به اندازه ای باشد که دشمن خیال هیچ نوع تجاوزی نداشته باشد. و به این باور برسد که اگر نتیجه تجاوز علیه کشوری مرگ نباشد، حداقل دست تجاوزگر را خواهد شکست.

بررسی محیطی تحقیق، وظایف و کارکردها

جنگ و دفاع الکترونیکی در پدافند غیرعامل وظیفه دارد با به کارگیری عناصر اطلاعاتی و عملیاتی خود در مناطق مختلف کشور، تهدیدات الکترونیکی و هرگونه حساسه‌ای به صورت عامل و غیرعامل را بشرح زیر شناسایی نماید:

- الف- جمع‌آوری اخبار از سامانه‌های الکترونیکی، حساسه‌ای و رایانه‌ای، تجهیزات الکترونیکی کشورهای هم‌جوار
- ب- جمع‌آوری اخبار از کلیه رسانه‌های گروهی الکترونیکی و ماهواره‌ای کشورهای هدف (وسایل ارتباط جمعی).
- جمع‌آوری اخبار فنی از سامانه‌ها و جنگ افزارهای الکترونیکی و حساسه‌ای کشورهای هدف.

بعد از مرحله شناسایی می‌توان با به کارگیری امکانات نیروی انسانی و تجهیزاتی یگان‌های تابعه خود به صورت عامل و غیر عامل، علیه هرگونه سامانه، حساسه و جنگ‌افزار الکترونیکی کشورهای هدف بنابه دستور به شرح زیر اقدام نماید:

۱- اجرای اختلال بر روی شبکه‌ها، سامانه‌های ارتباطی، غیر ارتباطی، حساسه‌ای و تجهیزات الکترونیکی کشورهای هدف.

۲- اجرای عملیات فریب (جعلی، تقلیدی) علیه سامانه‌های ارتباطی و غیرارتباطی و الکترونیکی کشورهای هدف.

۳- انجام شبیه‌سازی هدف‌ها، حساسه‌ها و تجهیزات الکترونیکی در سطوح تاکتیکی، عملیاتی و استراتژیکی نیروهای خودی جهت گمراه ساختن سامانه‌های جنگ الکترونیکی و سایر نیروهای اطلاعاتی کشورهای هدف.

تأمین

حوزه‌ی جنگ الکترونیک در خصوص تأمین نیازمندی‌های اقدامات عامل و غیرعامل سامانه‌های ارتباطی و غیر ارتباطی و به کارگیری حساسه‌ها، رایانه‌ها و تجهیزات الکترونیکی نیروهای خودی، وظایف زیر را بر عهده دارد:

الف- ارایه نظرات مشورتی در بومی سازی و بهینه سازی حساسه‌ها و تکنیک‌های پدافند الکترونیکی انواع تجهیزات و جنگ افزارهای عملیاتی-رزمی نیروهای مسلح و ارتقای سطح آموزش سامانه‌های الکترونیکی و حساسه‌ای تجهیزات متناسب با تهدیدات بالفعل و بالقوه جهت مراکز فرهنگی، تحقیقاتی.

ب- شرکت در رزمایش‌ها و تعیین نقاط ضعف و قوت الکترونیکی به صورت عامل و غیرعامل با بهره‌گیری از فرصت‌ها و تهدیدات الکترونیکی کشورهای هدف (منطقه‌ای و فرامنطقه‌ای).

پ- مطالعه سامانه‌های الکترونیکی، حساسه‌ای و تجهیزات الکترونیکی به کار گرفته شده توسط یگان‌های عمل‌کننده، پدافندی و آفندی و گزارش نقاط قوت و ضعف آن‌ها به مبادی ذی‌ربط.

ت- ارزیابی فنی و کاربردی بودن سامانه‌ها، حساسه‌ها و تجهیزات الکترونیکی نوین و تعیین آسیب‌پذیری سامانه‌های موصوف.

ث- تهیه طرح‌های پوشش الکترونیکی و اجرای آن در مناطق مختلف کشور.

ج- کنترل فعالیت کلیه سامانه‌ها، حساسه‌ها و تجهیزات الکترونیکی کشورهای هدف و اجرای اقدامات جنگ الکترونیک مناسب.

چ- تهیه طرح‌های راهبردی، عملیاتی و تاکتیکی جنگ‌های الکترونیکی نیروهای مسلح براساس سناریوهای تهدیدات الکترونیکی دشمن.

آموزش

بعد مهم دیگر در جنگ الکترونیک، آموزش گسترده آن است که در زمینه‌های مختلف نظامی و فنی است و به کارگیری جنگ الکترونیک باید با شناخت مقدرات و محدودیت‌های رسته‌های مختلف و همچنین روش‌های غلبه بر اقدامات جنگ الکترونیک و سامانه‌های الکترونیکی و ارتباطی و ارتباطی دشمن، نیاز به کسب دانش و آگاهی از قابلیت‌ها و امکانات سامانه‌های الکترونیکی فناورانه آنان باشد.

آماد و پشتیبانی

توجه به سامانه‌های ارتباطی روز جهان و تغییر سامانه‌های الکترونیکی و الکتروپاتیکی کشورهای هدف، همگامی سامانه‌های جنگ الکترونیک را با آخرین دستاوردهای فناوری روز ایجاد می‌کند. اگر در تهیه تجهیزات نوین و بومی الکترونیکی تسامحی صورت پذیرد، عملاً کارایی عناصر جنگ الکترونیک کاهش یابد و کشور قادر نخواهد بود به اهداف و منظوره‌های خود در به کارگیری جنگ الکترونیک در کشور با سامانه‌های متناسب با پیشرفت تجهیزات و جنگ‌افزارهای مجهز به انواع تکنیک‌های تهاجم الکترونیکی کشورهای هدف، اصلی انکار ناپذیر است.

نگهداری و تعمیر

یکی دیگر از ابعاد مهم توسعه و فعالیت جنگ الکترونیک، انجام نگهداری و تعمیر است. سامانه‌های جنگ الکترونیک به دلیل شرایط انحصاری و محدودیت استفاده آنان در سطح کشور، نیازمند استفاده از رده‌های تعمیراتی اختصاصی و مسیرآمادی و تدارکاتی خاص می‌باشد.

عملیات

امروزه استفاده از سامانه‌های مخابراتی و الکترونیکی در همه شبکه‌های ارتباطی در جهان غیر قابل انکار است. واحدهای نظامی و غیرنظامی، بدون بهره‌گیری از سامانه‌های جدید و پیشرفته، امکان اجرای مأموریت نخواهند داشت؛ از این رو تلاش برای دستیابی به این سامانه‌های پیشرفته از یک طرف و تلاش کشورها و نیروهای رقیب و متعارض، برای کاهش و یا خنثی نمودن بهره‌برداری نیروی مقابل از سامانه‌های مشابه الکترونیکی، منشأ ظهور علم، هنر و فن جنگ الکترونیک است، با توجه به تهدیدات موجود، نیازمندی‌های کشورهای پیشرو به پشتیبانی جنگ الکترونیک در نواح عملیات آفندی، پدافندی و انسداد مرزهای داخلی ایجاب می‌نماید که کشور از پیشرفته‌ترین تجهیزات جنگ الکترونیک بومی بهره‌برد و چنین اقدامی، مشابه فعالیت‌های تحقیقاتی دانش هسته‌ای در حد توان بالقوه و بالفعل دانشمندان ایرانی می‌باشد.

محورهای اساسی تغییر ساختار

بخشی از محورهای تغییر ساختار که به عنوان محورهای اساسی و اصلی تغییرها مطرح و مورد ارزیابی قرار گرفته عبارتند از:

۱- محور اطلاعات

امروزه اطلاعات علاوه بر ابعاد چهارگانه زمین، هوا، دریا و فضا، به عنوان بعد پنجم مطرح گردیده است. برتری در این بعد لازمی به کارگیری انواع روش‌های تولید اطلاعات است. این تولید اطلاعات از دیرباز مورد توجه انسان‌ها و طراحان عملیات نظامی است و امروزه نیز یکی از مهمترین عوامل پشتیبانی در بهره‌برداری از این اطلاعات می‌باشد؛ از طرف طراحان اطلاعاتی نیز روش‌های نوینی جهت جمع‌آوری و تولید اطلاعات مورد نیاز یگان‌های رزمی و

پشتیبانی رزمی الکترونیکی در جمع‌آوری و تولید اطلاعات است؛ از همین رو براساس تدابیر روز با به کارگیری عناصر جنگ الکترونیک در صدد دستیابی به روش‌های جمع‌آوری و تولید اخبار الکترونیکی بر آمده که مهم ترین اهداف به کارگیری روش‌های مزبور عبارتند از:

- جمع‌آوری اطلاعات الکترونیکی به علت ساختار سامانه‌ها و مقدرات آنها به عمق بیشتری از منطقه‌ی دشمن دسترسی پیدا می‌نماید؛ به گونه‌ای که این عمق گاهی به منازل و دفاتر خصوصی فرماندهان و رؤسای حکومتی و مملکتی نیز گسترش می‌یابد و حتی بسیاری از طرح‌ها قبل از هرگونه اقدامی، کشف و نیروی مقابل در صدد اقدامات تأمینی در برابر آنان بر می‌آید.

بر این اساس هر کشوری باید قادر باشد اطلاعات الکترونیکی کشورهای هدف را جمع‌آوری و بر پایه اطلاعات به دست آمده به استعداد، گسترش، نقاط ضعف و قوت، آموزش، لجستیک و ترکیب آنان دسترسی پیدا نماید.

- با به کارگیری امکانات مختلف، اخبار فنی را جمع‌آوری و با ترکیب آن با اخبار تاکتیکی، اطلاعات فناورانه و فناوری‌های الکترونیکی جدید کشورهای هدف را جمع‌آوری و بر پایه‌ی اطلاعات حاصله به فناوری‌ها، تجهیزات، مقدرات، محدودیت‌های فنی کشورهای هدف نفوذ کند.

- قادر باشد با استفاده از جنگ الکترونیک و عناصر جمع‌آوری کننده اخبار فنی و تاکتیکی را با اخبار سایر عناصر جمع‌آوری کننده اخبار تلاقی دهد.

- قادر باشد با به کارگیری گروه‌ها و رصدهای تجزیه و تحلیل به اطلاعات نهفته کشورهای هدف شامل تاکتیک، طرح‌های آتی و خط مشی عملیاتی، تجهیزاتی کشورهای هدف دست پیدا نماید.

- قادر باشد به طور کلی تهدیدات الکترونیکی، فنی و عملیاتی منطقه را مشخص و بر همین اساس با پیش بینی یگان‌های ESM فنی و عملیاتی نسبت به جمع‌آوری اخبار مربوطه اقدام کند و با تشکیل عناصر تجزیه و تحلیل در گروه جنگ الکترونیک به این فعالیت‌ها در جهت مورد نظر طراحان عملیات اطلاعاتی حرکت نمایند.

یافته‌های تحقیق

امروزه، کمتر کشوری و فناوری دیده می‌شود که از تجهیزات و سامانه‌های الکترونیکی به طور مستقیم برخوردار نباشد و یا به طور غیر مستقیم سامانه‌های الکترونیکی در بهره‌برداری موثر آنها نقش اصلی را ایفا ننماید. این وابستگی شدید تسلیحات نظامی به صنایع الکترونیک، عملیات را نیز متحول ساخته است. از یک طرف حضور سامانه‌های الکترونیکی با افزایش دقت و سرعت عمل به کمک فرماندهان آمده و از طرف دیگر آسیب‌پذیری این سامانه‌ها خود معضل و مشکلی در پیش روی مسؤولان قرار گرفته است؛ از این رو جنگ الکترونیک نقش بسزایی را در جهت کاهش و یا حذف آسیب‌پذیری، را ایفا می‌نماید.

محور مدیریت و کنترل

قادر باشد با به کارگیری سامانه‌های الکترونیکی، (ارتباطی، و غیر ارتباطی) اشراف الکترونیکی مسؤولان و فرماندهان و را از منطقه بحرانی ارتقا بخشد. با استفاده از سامانه‌های الکترونیکی سرعت و دقت را در روند عملیات جاری سازد.

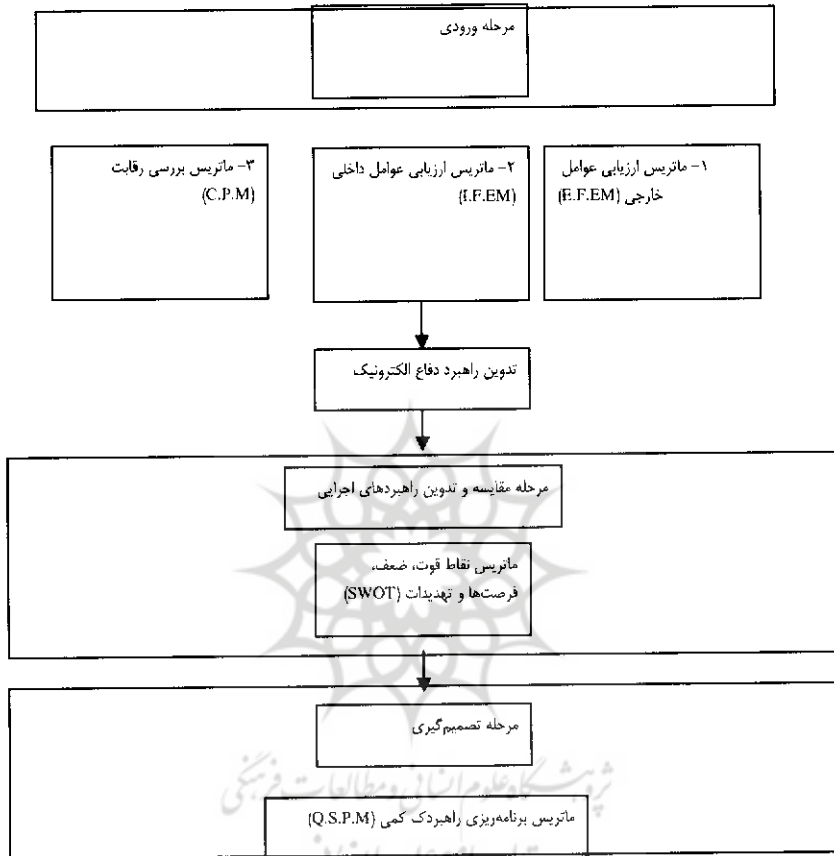
تجهیزات الکترونیکی به عنوان ابزار کنترلی مدیران، توان وی را در ابلاغ و کنترل اجرای به موقع فرامین خود در صحنه ی بحران تقویت نماید. تجهیزات بکارگرفته شده الکترونیکی و الکترواپتیکی قدرت رزمی عناصر آفندی را ارتقاء بخشد.

با استفاده از سامانه الکترونیکی، فرمانده قادر باشد در هر زمان با توجه به اطلاعات زنده (REAL TIME) از منطقه، تحلیل صحیحی از میدان عملیات به دست آورده و تصمیمات واقعی را اتخاذ نماید.

تجزیه و تحلیل داده‌ها

فرآیند تدوین راهبرد دفاع الکترونیکی:

روش تدوین راهبرد جنگ‌های الکترونیکی در کشور در یک چارچوب یا الگوی تصمیم‌گیری سه مرحله‌ای، به شرح زیر ارائه می‌گردد (اعرابی) - ۱۳۷۹-۳۲۵



محور مخابرات و ارتباطات:

اگرچه این محور به صورت ضمنی در سایر محورها مورد توجه بوده و در محورهای فرماندهی و کنترل به بخشی از آن نایل آمده و یا در محور اطلاعات نیز به بخشی دیگر از آن دسترسی پیدا کرده است، اما در ساختار جدید جنگ الکترونیک مخابرات به ارسال و دریافت هرگونه پیام (خبر) صوتی، تصویری، نوشتاری و ... از

طریق یکی از وسایل مخابره شامل شبکه‌های باسیم، بی سیم و امر بری اطلاق می‌شود و نیل به این تعاریف در کشور از اهمیت خاصی برخوردار است.

محور تجهیزات

تجهیزات الکترونیکی

یکی دیگر از ابعاد تغییر ساختار جنگ الکترونیک، نقش تعیین کنندگی جنگ الکترونیک در طراحی و ساخت انواع تجهیزات و ادوات نظامی و غیر نظامی مور نیاز می‌باشد. تا پیش از این در طراحی سامانه‌ها صرفاً حجم و وزن، مورد نظر قرار گرفت، ولی امروزه جنگ الکترونیک به گونه‌ای پارامترهای سامانه‌ها و طراحی آنها را متحول می‌سازد که کمتر طراح سامانه‌ای بدون اطلاع از پارامترهای جنگ الکترونیک اقدام به طراحی و ساخت سامانه‌ها و تجهیزات الکترونیکی می‌نماید.

محور آمادگی رزمی

یکی دیگر از محورهای تغییر ساختار جنگ الکترونیک، لزوم آمادگی رزمی یگان‌های عملیاتی است. اگرچه این آمادگی رزمی از کاربرد رزم انفرادی در محیط رزم (رزمایش) تا به کارگیری سلاح‌ها، موشک‌ها و انواع تسلیحات می‌باشد، ولی در مطالعه‌ی روند تهدیدات جنگ الکترونیک کشورهای هدف، جایگاه ویژه‌ای را به خود اختصاص داده است و با توجه به تنوع و پیچیدگی جنگ الکترونیک، در شرایط واقعی لازم است نهادهای مسؤوّل پیش از هرگونه حضور در شرایط واقعی، آمادگی لازم را در محیط‌های آموزشی، آزمایشگاهی و رزمایش‌ها کسب نمایند و به نهادهای مسؤوّل در کشور معرفی شوند و آموزش مقابله با آنان را در سطوح مرتبط گسترش دهند.

با بهره‌گیری از ماتریس ارزیابی عوامل محیط بیرونی، می‌توان عوامل اقتصادی، اجتماعی- فرهنگی، بوم شناسی، محیطی، سیاسی، دولتی، نظامی، فناوری را در زمینه سامانه‌های جنگ الکترونیکی با بهره‌گیری از سایر آگاهی‌های شهودی، کشورهای هدف (کشورهای تهدیدکننده امنیت ملی) را مورد ارزیابی قرارداد.

در زیر به مواردی از عوامل خارجی اشاره شده است:

۱. روابط سیاسی بین کشورهای همسایه، منطقه و فرمانطقه‌ای
۲. اوضاع سیاسی- نظامی منطقه‌ای و فرمانطقه‌ای

۳. شرایط جغرافیایی (ژئوپولوتیک و ژئوراهبردک منطقه)
۴. سامانه‌های آفندی کشورهای همسایه، منطقه‌ای و فرامنطقه‌ای
۵. شرایط اقتصادی و سهم اقتصاد دفاعی کشورهای هدف
۶. امکانات و مقدورات جنگ الکترونیکی کشورهای هدف.
۷. دیدگاه‌ها و نظریه‌ای کشورهای هدف در مورد جنگ الکترونیک.
۸. توان آفندی و پدافندعامل کشورهای هدف.
۹. ساختار سامانه‌ی جنگ الکترونیک کشورهای هدف در مجموعه ساختار سازمانی آنها.

با استفاده از جدول ترجیحات زیر، نتیجه نظریه‌های صاحب نظران جنگ الکترونیک آجا با بهره‌گیری از تکنیک A.H.P عوامل کلیدی خارجی جنگ الکترونیک آجا، مقایسه زوجی شده‌اند، که در جداول بعدی آورده شده است.

مقدار عددی	مقدورات جنگ الکترونیکی خودی و کشورهای هدف در آفند پدافند عامل و غیرعامل
۱	برابر
۳	کمی برتر
۵	برتر
۷	خیلی برتر
۹	قویاً برتر

شکل ۳ جدول ترجیحات و اعطای امتیاز

عوامل خارجی	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1.00	1.00	0.58	1.73	1.73	0.45	0.19	0.45	0.19	0.45	0.38	0.45	0.45
2	1.00	1.00	0.38	1.73	1.73	0.45	0.33	0.45	0.38	0.58	0.58	0.58	0.58
3	1.73	2.65	1.00	3.00	3.00	3.00	0.33	0.45	0.38	2.24	1.00	1.00	1.00
4	0.58	0.58	0.33	1.00	1.00	0.45	0.19	0.45	0.22	0.45	0.22	0.38	0.45
5	0.58	0.58	0.33	1.00	1.00	0.45	0.33	0.45	0.22	0.58	0.45	0.45	0.45
6	2.24	2.25	0.33	2.24	2.24	1.00	0.33	0.45	0.26	1.73	0.26	0.45	0.58
7	5.20	3.00	3.00	5.20	3.00	3.00	1.00	0.45	1.73	6.71	3.00	3.00	3.00
8	2.24	2.24	2.24	2.24	2.24	2.24	2.24	1.00	1.00	5.92	1.00	1.00	1.00
9	5.20	2.65	2.65	4.58	4.58	3.87	0.58	1.00	1.00	2.65	1.73	2.24	1.73
10	2.24	1.73	0.45	2.24	1.73	0.58	0.15	0.17	0.38	1.00	1.00	1.00	1.00
11	2.65	1.73	1.00	4.58	2.24	3.87	0.33	1.00	0.58	1.00	1.00	1.73	2.24
12	2.24	1.73	1.00	2.65	2.24	2.24	0.33	1.00	0.45	1.00	0.58	1.00	1.00
13	2.24	1.73	1.00	2.24	2.24	1.73	0.33	1.00	0.58	1.00	0.45	1.00	1.00
14	2.24	1.73	1.73	2.24	1.73	1.73	0.33	1.00	0.45	0.58	0.58	0.58	0.58
15	2.65	2.24	1.00	2.24	2.24	2.24	0.45	1.00	1.00	1.00	1.00	1.00	1.73
16	2.24	1.00	0.45	2.24	1.73	1.73	0.58	0.38	0.45	0.45	0.45	0.58	0.58
17	3.00	3.00	3.00	3.00	3.00	3.00	1.73	1.00	0.45	1.73	1.73	2.24	2.24

شکل ۴ جدول مقایسات زوجی عوامل خارجی توسط AHP

عوامل خارجی	1	2	3	4	5	6	7	8	9	10	11	12	13
1	0.03	0.03	0.03	0.04	0.05	0.01	0.02	0.04	0.02	0.02	0.02	0.02	0.02
2	0.03	0.03	0.02	0.04	0.05	0.01	0.03	0.04	0.04	0.02	0.04	0.03	0.03
3	0.40	0.09	0.05	0.07	0.08	0.09	0.03	0.04	0.04	0.08	0.06	0.05	0.05
4	0.01	0.02	0.02	0.02	0.03	0.01	0.02	0.04	0.02	0.02	0.01	0.02	0.02
5	0.01	0.07	0.02	0.02	0.03	0.01	0.03	0.04	0.02	0.02	0.03	0.02	0.02
6	0.06	0.10	0.02	0.05	0.06	0.03	0.03	0.04	0.03	0.06	0.02	0.02	0.03
7	0.13	0.07	0.15	0.12	0.08	0.09	0.10	0.04	0.18	0.23	0.19	0.16	0.15
8	0.06	0.09	0.11	0.05	0.06	0.07	0.23	0.09	0.10	0.20	0.06	0.12	0.05
9	0.13	0.06	0.13	0.10	0.12	0.12	0.06	0.09	0.10	0.09	0.11	0.05	0.09
10	0.06	0.06	0.02	0.05	0.05	0.02	0.02	0.01	0.04	0.03	0.06	0.09	0.05
11	0.07	0.06	0.05	0.10	0.06	0.12	0.03	0.09	0.06	0.03	0.06	0.09	0.11
12	0.06	0.06	0.05	0.06	0.06	0.07	0.03	0.09	0.05	0.03	0.04	0.05	0.05
13	0.06	0.06	0.05	0.05	0.06	0.05	0.03	0.09	0.06	0.03	0.03	0.05	0.05
14	0.06	0.06	0.08	0.05	0.05	0.05	0.03	0.09	0.06	0.02	0.04	0.03	0.03
15	0.07	0.07	0.05	0.05	0.06	0.07	0.05	0.09	0.10	0.03	0.06	0.05	0.09

شکل ۵ جدول نرمالیزه مقایسات زوجی عوامل خارجی توسط AHP

وزن نرمال	وزن غیر نرمال	عوامل خارجی
0.026	0.45	1
0.031	0.53	2
0.058	0.99	3
0.022	0.37	4
0.024	0.41	5
0.037	0.63	6
0.126	2.14	7
0.089	1.52	8
0.106	1.80	9
0.048	0.81	10
0.072	1.23	11
0.056	0.95	12
0.053	0.90	13
0.049	0.84	14
0.065	1.11	15
0.038	0.65	16
0.099	1.68	17

شکل ۶ جدول وزن عوامل خارجی توسط AHP

نتیجه گیری

اصول و ملاحظات راهبردی ناشی از بررسی میدانی نشان‌دهنده‌ی ضرورت توجه جدی به پدافند غیرعامل با تأکید بر اقدامات جنگ الکترونیک در سازکارهای زیر است:

- ۱- ایجاد تناسب سامانه و تجهیزات با تجهیزات سازمانی، سیاست‌های دفاعی و راهبرد نظامی کشور.
- ۲- وجود تناسب سامانه‌ها و تجهیزات جنگ الکترونیک با توان اقتصادی و قابلیت‌های تولیدی و صنعتی کشور.
- ۳- وجود تناسب و هماهنگی سامانه‌ها و تجهیزات جنگ الکترونیک با سیاست‌های ملی ج.ا.ا در منطقه و جهان.
- ۴- تطبیق سامانه‌ها و تجهیزات جنگ الکترونیک با توانایی‌های بالقوه و بالفعل (نیروی انسانی - آموزش - سازمان - نگهداری - تعمیرات و ...)

- ۵- تطبیق سامانه‌ها و تجهیزات جنگ الکترونیکی با شرایط اقلیمی متنوع کشور.
 - ۶- تطبیق و همخوانی سامانه‌ها و تجهیزات جنگ الکترونیکی با شرایط آب و هوایی کشور.
 - ۷- توان مقابله و پایداری در برابر تجهیزات جنگ الکترونیکی سامانه‌های جنگ‌افزاری کشورهای هدف.
 - ۸- ایجاد یکنواختی و همگونی فرهنگ جنگ الکترونیکی در حد ممکن در کشور.
 - ۹- پرهیز از تنوع بیش از حد تجهیزات جنگ الکترونیکی در کشور.
 - ۱۰- اتکا بیشتر به تولید داخلی و پرهیز از وابستگی جنگ الکترونیکی به خارج.
 - ۱۱- امکان تأمین تجهیزات جنگ الکترونیکی مناسب از منابع مختلف.
 - ۱۲- جلوگیری از وارد شدن در یک مسابقه‌ی تسلیحاتی و جنگ الکترونیکی در منطقه تا حد ممکن.
 - ۱۳- قابلیت اعتماد منابع جنگ الکترونیکی در زمان جنگ و بحران‌ها و اندیشیدن تمهیدات لازم در این زمینه.
 - ۱۴- مد نظر قراردادن روند پیشرفت‌های فناوری در تکمیل طرح‌های جنگ الکترونیکی.
- انواع تجهیزات سامانه‌های جنگ‌های الکترونیکی، توانایی نسبی تأمین اطلاعات اهداف زیر را در کشور دارند:**
- ۱- مراقبت از حفظ صلح در مواقع عادی، از طریق جمع‌آوری اطلاعات به منظور جلوگیری از هرگونه غافلگیری.
 - ۲- بر آورد تهدیدات تاکتیکی، عملیاتی و راهبردی خاص جنگ الکترونیکی کشورهای هدف، با ضریب اطمینان بالا.
 - ۳- اعلام هشدار و ارائه‌ی عکس‌العمل مناسب.
 - ۴- حضور موثر در درگیری‌ها با هدف کسب برتری در آفتد و پدافند الکترونیکی.

۵- ایجاد توازن در مسائل دیپلماسی، اقتصادی، اجتماعی-فرهنگی و نظامی بین کشورها در صحنه روابط بین‌الملل، از طریق کسب اطلاعات لازم از کشورهای هدف به منظور تقویت مؤلفه‌های قدرت در همه زمینه‌ها.

چشم‌انداز دفاع عامل و غیر عامل الکترونیکی

امروزه روند توسعه تکنیک‌ها و فناوری‌های جنگ الکترونیکی با شتابی بیش از هر زمان دیگر همچنان رو به تکامل است. ظهور روش‌ها و تکنیک‌های جدید با بهره‌گیری از تجهیزات و سایر فناوری‌های نوین پرقدرت و حساس تر در حوزه امواج الکترومغناطیسی، آسیب‌پذیری‌ها را در بین کشورها در ابعاد گوناگون افزایش داده است.

تبدیل حوزه‌های آنالوگ به دیجیتال با استفاده از مدارهای نیمه هادی، هیبریدی و غیره از یکسو و نرم افزار و تکنیک‌های هوش مصنوعی جهت اعمال مدیریت مطمئن‌تر و تفسیر اطلاعات از سوی دیگر که تا چندین سال پیش به طور کلی غیرقابل تصور بود، تکنیک‌ها و فناوری جنگ الکترونیکی را پویاتر ساخته است و در اختیار داشتن چنین شرایطی چشم‌انداز سامانه‌های جنگ الکترونیکی آجا، دستیابی به تجهیزات و فناوری‌های نوین جنگ الکترونیکی و در اختیار داشتن نیروی انسانی متخصص و واجد شرایط در شبکه فرماندهی و کنترل کشور به منظور پشتیبانی مقتدرانه از عملیات‌های آفندی و پدافندی کشور در مقابله با تهدیدات دشمن در زمان صلح و جنگ می‌باشد.

در این راستا، هدف و محور توجه سامانه‌های جنگ الکترونیکی آجا شامل موارد زیر است:

- ۱- پاسخ‌گویی مناسب به نیازها و درخواست‌های پدافند عامل و غیرعامل در کشور در زمینه‌ی ارائه عملیات جنگ‌های الکترونیکی متناسب با قابلیت‌های تجهیزاتی و مهارت‌های انسانی در نیروهای سه‌گانه.
- ۲- بهبود مستمر کیفیت عملیات جمع‌آوری اطلاعات، تهاجم الکترونیکی و پدافند الکترونیکی در پشتیبانی از مأموریت‌های محوله به نهادهای مسؤول در زمان صلح و جنگ.

- ۳- تأکید به افزایش مهارت‌های انفرادی و کار گروهی کاربران انواع تجهیزات جنگ الکترونیکی سامانه‌ها و تجهیزات آفندی و پدافندی در شبکه فرماندهی و کنترل.
- ۴- تلاش در جهت ایجاد مراکز تحقیق و توسعه جدید در زمینه‌ی جنگ‌های الکترونیکی، به منظور دستیابی به تکنیک‌ها و فنون نوین جنگ الکترونیکی جهت پشتیبانی از عملیات‌های آفندی. پدافندی نیروهای سه گانه در زمان صلح و جنگ و تحقق خودکفایی دفاعی در این زمینه.



۱. جاوید، روح ا... - ۱۳۷۴، «آیا سامانه های جنگ الکترونیک هوپیمای اف-۴ (حفاظت از خود) جواب گوی نیاز عملیاتی می باشد؟»، پایان نامه کارشناسی ارشد، دافوس آجا.
۲. فیلیپونری، سامانه های دفاع الکترونیکی، ترجمه: سیاسی سید محسن و غفاری مهید، ۱۳۷۵ نهاجا.
۳. مرکز مطالعات و برنامه ریزی راهبردی موسسه آموزشی و تحقیقاتی صنایع دفاع وزارت دفاع و پشتیبانی نیروهای مسلح - ۱۳۷۹، «راهبرد امنیت ملی جمهوری اسلامی ایران بایسته های پژوهشی».
۴. محمودزاده، ابراهیم - ۱۳۸۰، «تدوین الگوی راهبرد توسعه فناوری دفاعی» (پایان نامه)، دانشگاه عالی دفاع ملی، دانشکده مدیریت راهبردی.
۵. جواهری، علی رضا - ۱۳۷۹، «اقدامات جنگ الکترونیکی» دانشگاه هوایی شهید ستاری.
۶. فیلیپونری، ترجمه سیاسی سید محسن و غفاری مهید - ۱۳۷۹، «سامانه های دفاع الکترونیکی».
۷. ستاریخواه، علی، بهار - ۱۳۷۷، «تاثیر جنگ الکترونیک و سامانه های مربوط به آن بر راهبرد پدافند هوایی در دهه های آینده»، همایش قرارگاه خاتم الانبیاء.
۸. نقشینه، نادر - ۱۳۷۶، «جنگ سیبرنتیکی و پنجره آسیب پذیری»، مرز اطلاع رسانی و خدمات علمی وزارت جهاد سازندگی.
۹. صفی خانی، علی - ۱۳۷۵، «نقش جنگ الکترونیک در عملیات نظامی»، پایان نامه کارشناسی ارشد، دافوس.
۱۰. ساعتی، توماس ال، ترجمه قدسی پور سید حسن، ۱۳۷۸، «تصمیم گیری چند معیاره فرآیند تحلیلی سلسله مراتبی»، مرکز نشر دانشگاه صنعتی امیرکبیر.

۱۱. نادری، علی محمد؛ ۱۳۷۸، «راهبرد نهاجا در به کارگیری جنگ الکترونیک چه گونه باید باشد؟»، پایان نامه دکترای علوم راهبردک، د.ا.ع.
۱۲. دفتر مطالعات موسسه آموزشی و تحقیقاتی ودجا، ۱۳۷۹، «شیوه طراحی راهبرد دفاعی برای دهه های آینده».

۱۳. Bray's, electronic warfare.
۱۴. Curtis shleher, introduction to electronic warfare.
۱۵. c.hax&s.majiuf, ۱۹۹۹, the strategy concept and process a pragmatic approach.
۱۶. Done e.gordon, ۱۹۸۱. electronic warfare element of strategy and multiplier of combat power.
۱۷. Filiponeri, introduction to electronic warfare defence system.
۱۸. Richard j.wiegand, radar electronic countermeasure system design.
۱۹. The café royal, London UK, electronic warfare air, land& seam conference & exhibition, April ۱۹۹۶
۲۰. Van brunt, applied E.C.M, VOLUME۲.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی