

دوفصلنامه پژوهش‌های مدیریت و فرماندهی نظامی
دانشگاه افسری و تربیت پاسداری امام حسین (ع) - دانشگاه امیرالمؤمنین (ع) نرسا
سال هجدهم، شماره ۵۴، پاییز و زمستان ۱۴۰۲ صص ۱۰۳-۸۳

جنگ الکترونیک و ملاحظات آن در یگان‌های پیاده و تکاور

مهدی حسینی^{۱*}، مجتبی ناصحی^۲

تاریخ دریافت: ۱۴۰۲/۰۷/۱۷ تاریخ پذیرش: ۱۴۰۲/۱۱/۱۹



چکیده

جنگ الکترونیک یا همان جنگال از چهار بخش اصلی حفاظت الکترونیکی، تهاجم الکترونیکی، پشتیبانی الکترونیکی و اطلاعات سیگنال تشکیل شده است که این بخش‌ها در کنار یکدیگر با استفاده از امواج الکترومغناطیس اقدام به شنود، فریب، اختلال، جهت‌یابی و مکان‌یابی دشمن نموده و با انجام این اقدامات به اطلاعات ارزشمندی از دشمن مانند ترکیب، گسترش، استعداد، سازمان، ویژگی‌ها و توانایی‌های یگان و فرماندهان آن‌ها دست می‌یابد. در مقابل جنگال دشمن نیز دارای قابلیت‌های مشابه و حتی بیشتر می‌باشد و می‌تواند با انجام اقدامات جنگال بر تجهیزات و سلاح‌ها و ارتباطات یگان‌های پیاده مانند جی‌پی‌اس‌ها، بی‌سیم‌ها، کوادکوپترها، پهپادها، سلاح‌های هوشمند ضد زره و بالگرد تأثیر منفی گذاشته و در عملکرد آن‌ها اختلال ایجاد نماید؛ لذا لازم است هر نیروی پیاده و تکاور آشنایی لازم را با جنگ الکترونیک داشته، نقاط قوت و ضعف تجهیزات خود را در برابر جنگ الکترونیک بداند و با اقدامات لازم برای مقابله با جنگ الکترونیک دشمن آشنا باشد و استفاده حداکثری را از جنگال خودی در عملیات خود داشته تا با استفاده از این توانمندی در کنار سایر توانمندی‌ها بتواند ابتکار عمل را در میدان نبرد در دست بگیرد. با توجه به مباحث مطرح شده در این مقاله سعی بر آن است که یک نیروی پیاده تکاور به طور اجمالی با جنگال و توانمندی‌های آن آشنا شود.

^۱ فراگیر دوره عالی دوم جنگال دانشکده علوم و فنون پیاده و تکاور، دانشگاه علوم و فنون امیرالمؤمنین علیه السلام.

^۲ مدرس دانشگاه افسری و تربیت پاسداری امام حسین علیه اسلام.

واژه‌گان کلیدی: جنگ الکترونیک، امواج الکترومغناطیسی، حفاظت الکترونیکی، پشتیبانی الکترونیکی، تهاجم الکترونیکی.

مقدمه

تاریخ چند ساله اخیر نشان می‌دهد که جنگ الکترونیک همواره در طول دوره‌های مختلف دستخوش جهش‌های ناگهانی گردیده است که این امر نتیجه غافلگیری توسط سلاح‌ها و تجهیزات ناشناخته دشمن بوده که این سلاح‌ها و تجهیزات برای هدایت و کنترل از قسمتی از طیف الکترومغناطیس بهره می‌بردند (طلعتی، اصلی نژاد، ۱۳۹۶: ۷). امروزه تجهیزات مرتبط با جنگ الکترونیک بر روی هواپیماهای نظامی، ناوها، موشک‌ها و سامانه‌های پدافندی، خودروهای زرهی و تاکتیکی، پهپادها و بالگردها نصب می‌شود که این اقدام نشانه حضور جنگ الکترونیک در تمام حوزه‌های نظامی می‌باشد. در گذشته جنگ الکترونیک تنها شامل ایجاد اختلال در ارتباطات رادیویی دشمن و شنود گفتگوهای دشمن بود؛ ولی کاربردهای نوین دیگری مانند هدایت نفرات و موشک‌ها، ایجاد اختلال در عملکرد سامانه‌های پدافندی، هواپیماهای جنگنده و شناسایی، پهپادها، بالگردها، موشک‌ها و ماهواره‌ها و تجهیزات ناوبری به جنگ الکترونیک اضافه شده است.

بیان مسئله

موفقیت یک نیروی نظامی در صحنه نبرد به عوامل متعددی بستگی دارد که یکی از مهم‌ترین این عوامل به‌کارگیری تجهیزات و تاکتیک‌های متناسب با تکنولوژی و دانش تجهیزاتی نیروی دشمن مقابل است. از جمله این تجهیزات و تکنولوژی‌هایی که امروزه دشمنان ما توجه ویژه‌ای به آن دارند جنگ الکترونیک می‌باشد. در این جا چند مسئله مطرح می‌شود از جمله اینکه:

- نقش و اهمیت جنگ الکترونیک در یگان‌های پیاده و تکاور چیست؟
- یگان‌های پیاده و تکاور چه ملاحظاتی را در برابر جنگ الکترونیک باید انجام دهند؟
- لازمه رسیدن به پاسخ این سؤالات تنها در شناخت جنگ الکترونیک و توانمندی‌های آن نهفته است.

اهمیت و ضرورت تحقیق

فرمانده معظم کل قوا حضرت آیت‌الله خامنه‌ای درباره جنگ الکترونیک این گونه می‌فرمایند: شما یکی از مسائلی که در آینده با آن مواجه هستید جنگال است بروید جنگال را در سازمان‌هایتان جدی بگیرید و روی آن کار کنید، کار تحقیقاتی و تولید بکنید، از هر جا می‌توانید به دست بیاورید و در جنگال صاحب فناوری باشید. اگر نداشته باشید دشمن که جنگ کرد تمام دستگاه‌های ارتباطی شما خاموش می‌شود، رادارها خاموش می‌شود، هواپیماها روی آسمان سرگردان می‌شوند. بدون جنگ الکترونیک در این فضا نمی‌توان ماند.

تنها با تأمل در این بیانات فرماندهی کل قوا می‌توان به اهمیت بسیار بالای توجه به مقوله جنگ الکترونیک در نیروهای مسلح پی برد. مسئله مهم‌تری نیز وجود دارد و آن این است که توجه به بحث جنگال تنها وظیفه واحدهای جنگال نبوده؛ بلکه یکایک نیروهای نظامی باید آشنایی لازم با آن را داشته تا بتوانند در برابر جنگال دشمن آسیب‌پذیری خود را به حداقل برسانند.

از آنجاکه یگان‌های پیاده و تکاور در صحنه نبرد در نزدیک‌ترین فاصله با دشمن درگیر می‌شوند و همچنین باتوجه به استفاده این نیروها تجهیزات و سلاح‌های الکترونیکی و الکتریکی مانند (پهپادها، کوادکوپترها، سلاح‌ها و موشک‌های هدایت‌شونده، وسایل ارتباطی و...) که تمامی آنها را می‌توان توسط جنگال مورد هدف قرارداد آشنایی یگان‌های پیاده و

تکاور با جنگال و ملاحظات آن ضرورت بسیار بالایی دارد؛ لذا نیروهای پیاده تکاور باید با جنگال آشنا شده تا با شناخت و رعایت ملاحظات آن و همچنین به‌کارگیری آن در مواقع لازم بتوانند در صحنه نبرد برتری را در دست گرفته، خود و تجهیزات را حفظ نموده و مأموریت را با کمترین تلفات به انجام برسانند و همچنین توان رزم خود را ارتقا بخشند.

پیشینه تحقیق

در دو دهه اخیر باتوجه به روشن شدن هر چه بیشتر نقش جنگ الکترونیک در مأموریت‌های نیروهای نظامی تحقیقات و پژوهش‌های گسترده‌ای در زمینه جنگ الکترونیک صورت گرفته است که از آن جمله می‌توان به کتاب‌هایی چون (جنگ الکترونیک، نایینی، محمدمهدی)، (اصول عملیات جنگ الکترونیک، موسوی، سید نواب، خداپرست، فاطمه)، (جنگ الکترونیک در مخابرات، جزی زاده کریمی، علیرضا، اذربر، علی)، (دکترین جنگ الکترونیک مشترک، موسوی، سید نواب)، (جنگ الکترونیک در مقابله با نسل جدید تهدیدات، بایوردی، فرخ، حسینی اژدری، سیدمحمد) اشاره نمود.

تاریخچه جنگال

از زمانی که ارتباطات رادیویی در جنگ به کار گرفته شد جنگ الکترونیک نیز شکل گرفته است. تکنیک‌های اولیه ابتدایی بودند؛ ولی از جنگ جهانی دوم صورت پیچیده‌تر و پیشرفته‌تری به خود گرفتند. اولین تلاش جنگ الکترونیک در سال ۱۹۰۵ میلادی بین روسیه و ژاپن گزارش شده است. بدین صورت که کشتی‌های ژاپنی ناوگان روس را تعقیب می‌کردند و حرکات و آرایشات آن‌ها را به فرماندهان بالاتر مخابره می‌کردند. فرانسه و اتریش جزء اولین کشورهایی بودند که به ارزش استراق سمع مخابرات رادیویی پی بردند. در سال ۱۹۰۸ میلادی زمانی که بر سر الحاق بوسنی و هرزگوین به اتریش بین ایتالیا و این کشور بحران

ایجاد شد اتریشی‌ها مخابرات رادیویی ایتالیایی‌ها را استراق سمع و کشف کردند. انگلیسی‌ها در سال ۱۹۱۵ میلادی برای اولین مرتبه یک سامانه سمت یاب به‌منظور استفاده علیه زیردریایی‌ها اختراع کردند. در سال ۱۹۱۷ میلادی فرانسویان اولین زاویه‌یاب بی‌سیم کوچک قابل حمل با خودرو را ساختند. آمریکایی‌ها هم که بیکار ننشسته بودند یک سال بعد وسایل سمت یاب قابل حمل را ساختند. ایران نیز اولین تجربه جنگال خود را در جنگ تحمیلی با انجام شنود شبکه‌های عراق آغاز نمود و این سرآغازی در جهت تحقیق و ساخت تجهیزات جنگال در نیروهای مسلح جمهوری اسلامی ایران بود (محمدی، ۱۳۸۷: ۱۱). به‌عنوان یکی از مهم‌ترین اقدامات واحدهای جنگال که بازتاب جهانی داشت می‌توان به حمله موشکی سپاه پاسداران انقلاب اسلامی به نیروهای تروریستی آمریکا در پایگاه عین الاسد اشاره نمود که در این عملیات جنگال به‌عنوان یکی از ارکان اصلی این عملیات با به‌کارگیری تکنیک‌های جنگ الکترونیک در کنار سایر اقدامات، سیستم‌های پدافندی ارتش متجاوز و تروریستی آمریکا را مختل نموده و پدافند آن‌ها را از کار انداختند که در نتیجه این اقدامات موشک‌ها به پایگاه اصابت نمود.

تعریف جنگ الکترونیک (EW)^۱

عملیات نظامی شامل به‌کاربردن انرژی الکترومغناطیس به‌منظور تشخیص، بهره‌برداری، کاهش و یا ممانعت از بکار بردن امواج الکترومغناطیسی توسط دشمن را جنگ الکترونیک یا به‌اختصار جنگال گویند (کالوندی، ۱۳۷۴: ۵۷).

بخش‌های اصلی جنگ الکترونیک

جنگال دارای دو بخش اصلی مخابراتی (COMINT) و غیر مخابراتی (ELINT) است.

^۱ Electronic Warfar

۱- بخش مخابراتی (COMINT)

دارای قدمتی به اندازه خود مخابرات الکترونیک بوده و به منابع مخابراتی که در باندهای (V/UHF-HF-SHF) کار می‌کنند اطلاق می‌شود. در آن شنود و تجزیه و تحلیل ارتباطات رادیویی معمولاً مهم‌تر از تشخیص مشخصات فرستنده است.

۲- بخش غیر مخابراتی (ELINT)

این بخش از زمان شکل‌گیری رادارها و سامانه‌های ناوبری در جنگ جهانی دوم توسعه پیدا کرد و معمولاً به سامانه‌های راداری در باند HF یا بالاتر اختصاص داده می‌شوند و در این بخش سنجش مشخصه‌های منبع انتشار امواج عامل اصلی است. (صنایع دفاع الکترونیک ۳:۱۳۸۶)

ساختار جنگ الکترونیک

در یک تقسیم‌بندی فلیپو نری^۱ در کتاب سیستم‌های دفاع الکترونیک جنگ الکترونیک را شامل پنج قسمت اصلی به شرح زیر می‌داند:

۱. جنگ اطلاعات^۲ (IW)

۲. حفاظت الکترونیکی^۳ (EP یا ECCM)

۳. تهاجم الکترونیکی^۴ (EA یا ECM)

۴. پشتیبانی الکترونیکی^۵ (ES یا ESM)

۵. اطلاعات سیگنال^۶ (SIGINT)

^۱ Fillipo Neri

^۲ Information War

^۳ Electronic Protection- Electronic Counter Counter Measures

^۴ Electronic Attack- Electronic Counter Measures

^۵ Electronic Support- Electronic Support Measuurs

^۶ Signal Intelligence

به‌طور کلی می‌توان جنگ الکترونیک را شامل چهار قسمت اصلی (SIGINT, EA, ES, EP) دانست.

تهاجم الکترونیکی (EA)

در گذشته به ECM معروف بوده است و بخشی از جنگ الکترونیک است که استفاده از انرژی الکترومغناطیس برای حمله به پرسنل، تجهیزات و امکانات به‌منظور کاهش عملکرد یا تخریب توان رزمی دشمن را در بر می‌گیرد و بخش آفندی جنگال بوده و شامل، اختلال یا همان جمینگ، فریب الکترونیکی و خنثی‌سازی هست.

اختلال یا جمینگ^۱

عبارت است از انتشار عمدی، انتشار مجدد یا انعکاس انرژی الکترومغناطیس به‌منظور اختلال، تخریب یا جلوگیری از استفاده دشمن از طیف انرژی الکترومغناطیس (امیر مصلح، ۱۳۸۸: ۵).

فریب^۲

به‌کارگیری انرژی الکترومغناطیس جهت القای اطلاعات غلط و گمراه‌کننده و یا انکار و تکذیب اطلاعات صحیح برای سیستم‌ها و تسلیحات الکترونیکی دشمن را گویند.

خنثی‌سازی

استفاده از سطوح بسیار بالای انرژی الکترومغناطیسی برای ازهم‌پاشیدن یا آسیب رساندن دائمی به تجهیزات الکترونیکی دشمن می‌باشد.

^۱Jamming-

^۲Deception

مانند سلاح‌های انرژی مستقیم (RFDEW)^۱، بمب‌های الکترومغناطیسی EMP^۲ و سلاح‌های مایکروویوی (HPMW)^۳ (صنایع دفاع الکترونیک ۱۳۸۶: ۵).

حفاظت الکترونیکی (EP)

در گذشته به (ECCM) معروف بوده است و فعالیت‌هایی را در بر می‌گیرد که برای حفاظت از کارکنان "امکانات و تجهیزات در برابر کلیه دستگاه‌های جنگ الکترونیک دشمن که باعث تنزل عملکرد یا خنثی شدن و یا خراب شدن تجهیزات رزمی نیروهای خودی شوند در نظر گرفته می‌شوند و بخش پدافندی جنگال می‌باشد (صنایع دفاع الکترونیک ۱۳۸۶: ۹).

پشتیبانی الکترونیکی (ES)

در گذشته به (ESM) معروف بوده است و تحت کنترل مستقیم فرمانده عملیات در پشتیبانی از فعالیت‌های شنود، شناسایی و تعیین محل منابع عمدی یا غیرعمدی پرتوهای الکترومغناطیسی بکار گرفته شده است. عمده وظیفه آن ارائه عملیات جاسوسی جهت فراهم‌سازی هدایت برای تهاجم الکترونیکی و راهنمایی کردن منابع تجسس و منابع آشکارسازی هدف می‌باشد. دارای بخش‌های (جستجو^۴، شنود^۵، جهت‌یابی و مکان‌یابی^۶، تجزیه و تحلیل^۷، تشخیص^۸ و پایش یا مانیتورینگ^۹) می‌باشد (صنایع دفاع الکترونیک ۱۳۸۶: ۱۹).

1. Radio Frequenc Directed Eneryj Weapons

2. Electronic Magnetic Pulse

3. High Power Microwave Weapons

4. Searching

5. Interception

6. Direction & Position Finding

7. Analyzing

8. Recognition

9. Monitoring

اطلاعات سیگنال (SIGINT)

بخشی از اقدامات جنگ الکترونیک است که وظیفه آشکارسازی، شناسایی و دسته‌بندی تهدیدات الکترونیکی و تمامی منابع انتشار الکترومغناطیس را در سطح استراتژیک بر عهده دارد. وظیفه اصلی سیستم‌های SIGINT شناسایی و کسب هر چه بیشتر اطلاعات در خصوص انتشارات الکترومغناطیس دشمن است. این سیستم‌ها عموماً به دودسته زیر تقسیم می‌شوند:

۱- جمع آوری اطلاعات الکترونیکی^۱ (ELINT)

۲- جمع آوری اطلاعات مخابراتی^۲ (COMINT)

ویژگی بارز اطلاعات سیگنال برخلاف عملیات‌های متداول نظامی که دربرگیرنده آموزش در زمان صلح و عملیات در زمان جنگ است، برای اطلاعات سیگنال هیچ موقع زمان صلح نداریم. معمولاً عملکرد یک سیستم SIGINT یک عملکرد استراتژیک محسوب می‌شود چرا که این‌گونه سیستم‌ها برای شناسایی توان نظامی، دفاعی و عملیاتی دشمن مورد استفاده قرار می‌گیرند (کالوندی، ۱۳۷۴: ۲۰۷).

مأموریت‌ها و توانمندی‌های جنگ الکترونیک

اهم توانمندی‌ها و مأموریت‌های واحدهای جنگ الکترونیک بدین شرح می‌باشد:

- شناسایی مراکز کنترل و فرماندهی
- انجام شنود کلیه لایه‌های ارتباطی
- جهت‌یابی تجهیزات، تأسیسات و سامانه‌های ارتباطی و همچنین مکان‌یابی آن‌ها - نفوذ و

^۱.Electronic Intelligence

^۲.Communication Intelligence-

انجام فعالیت‌های فریب در شبکه‌های بی‌سیم، ناوبری، راداری، هدایت موشک‌ها و...

– عملیات جمینگ یا اختلال هوشمند با استفاده از تکنیک‌ها و تاکتیک‌های مختلف با سامانه‌های مجهز شیلر اختلال، پهپادها، گلوله‌های یک‌بارمصرف، سایت‌های پرنده، سایت‌های دریایی یا شناور، بالگردها و بالون‌های مخابراتی، سایت‌های فضایی "ماهواره‌ها"

– استفاده از بمب‌های الکترومغناطیسی برای از بین بردن کلیه تجهیزات الکترونیکی و مدارات برقی

– پی‌بردن به گسترش، ترکیب، استعداد، آموزش‌ها، نحوه امداد رسانی، شایستگی‌های رزمی دشمن و...

اقدامات یگان‌های پیاده و تکاور در جنگ الکترونیک

این اقدامات را می‌توان به دو بخش تقسیم کرد:

۱. اقدامات در به‌کارگیری جنگال خودی

۲. اقدامات در مقابله با جنگال دشمن

اقداماتی که در به‌کارگیری جنگال خودی باید مورد توجه قرارداد از این قرار می‌باشد

– توجه نیروها نسبت به اهمیت و نقش تعیین‌کننده جنگال در نبردهای امروزی و آینده

– آموزش و آشنا نمودن نیروها با جنگال و توانمندی‌های آن

– استفاده حداکثری از قابلیت‌های جنگال در مأموریت‌ها

– هماهنگی بین فرمانده یگان پیاده و تکاور با فرمانده واحد جنگال در تمامی زمینه مانند شنود، اختلال، فریب و...

– اطمینان از سلامت و کارایی تجهیزات و سامانه‌های جنگال که می‌خواهیم استفاده کنیم

قبل از مأموریت‌ها با تست نمودن آن‌ها روی تجهیزات خودی مانند بی‌سیم، جی‌پی‌اس، رادیو، گوشی‌های همراه مختلف و...

- اعزام واحد جنگال قبل از اجرای مأموریت به منطقه مأموریت جهت پایش و رصد منطقه علاوه بر تیم‌های شناسایی که نیروی پیاده به‌صورت جداگانه به‌کارگیری می‌کند.

- استفاده از سامانه‌های اختلال کوادکوپتر مانند ارش و صیاد ۱۰۰ و... علیه کوادکوپترهای دشمن در سازمان رزم نیروهای پیاده و تکاور که قابل حمل توسط فرد بوده و بدون هیچ آسیبی کوادکوپتر را روی زمین نشاند تا بتوان از اطلاعات آنها بهره‌برداری نمود.

- استفاده از سامانه‌های انهدام کوادکوپتر مانند سامانه‌های لیزری که با شناسایی و قفل کردن روی کوادکوپتر در کمتر از چند ثانیه آن را به آتش کشیده و منهدم می‌کند.

- استفاده از سامانه‌های اختلال GPS^۱ و ماهواره‌ها در مأموریت‌ها با توجه به نیاز؛ مانند سامانه‌های قائم، ساتر، نجم و... که با استفاده مناسب از این سامانه‌ها می‌توان تمامی تجهیزات و تسلیحات دشمن را که هدایت و ناوبری آن‌ها توسط ماهواره‌ها و GPS انجام می‌گیرد و در برد این سامانه‌ها هستند جمینگ نمود. مانند (کوادکوپترها، پهپادها، بالگردها، جنگنده‌ها، هواپیماهای شناسایی، موشک‌ها، سامانه تشخیص دوست از دشمن و...)

- به‌کارگیری جمرهای خودرویی در ستون کشی‌های خودرویی جهت مقابله هرچه بیشتر با تله‌های انفجاری کنترل از راه دور

- به‌کارگیری جمر کوله‌ای (VIP) در حرکات و ستون کشی‌های پیاده که به‌راحتی توسط فرد حمل شده جهت مقابله هرچه بیشتر با تله‌های انفجاری کنترل از راه دور

اقدامات لازم در مقابله با جنگال دشمن

عمده اقداماتی که باید در برابر جنگال دشمن صورت داد مربوط به تجهیزات و تسلیحاتی

1. Global Positioning system

می‌شود که در یگان‌های پیاده مورد استفاده قرار می‌گیرند و می‌توانند مورد هدف جنگال دشمن باشند. در اینجا به طور مختصر به این اقدامات می‌پردازیم.

بی‌سیم

امروزه تاکتیک‌های نبرد یگان‌های پیاده و تکاور با گذشته متفاوت شده است و نیروهای پیاده دیگر به طور کلاسیک عمل نمی‌کنند و اغلب به صورت دسته‌های کوچک خود کافی و خوداتکا و سیال عمل می‌نمایند. این نحوه عمل مستلزم به‌کارگیری بیشتر وسایل ارتباطی به‌ویژه بی‌سیم می‌باشد؛ لذا باتوجه به این مطلب وجود یک ارتباط امن و کارآمد بین آن‌ها نقش حیاتی برای هماهنگی و انجام مأموریت آن‌ها ایفا می‌کند از طرف دیگر استفاده بیشتر از بی‌سیم برابر با آسیب‌پذیری بیشتر در مقابل جنگال دشمن می‌باشد. جنگال دشمن قادر است از طریق اقدامات جنگ الکترونیک در بحث ارتباطات ما اقداماتی مانند اختلال، فریب، شنود، جهت‌یابی و مکان‌یابی و... را در مدت‌زمان اندکی انجام دهد. باتوجه به مطالب بیان شده و اهمیت نقش ارتباطات بی‌سیم به شرح اقدامات لازم در ارتباطات بی‌سیم در برابر جنگال دشمن می‌پردازیم.

اقدامات لازم در ارتباط بی‌سیم در برابر جنگال دشمن

- استفاده از جدول نشانی
- استفاده از جداول رمز دستی و تغییرات به موقع آن‌ها
- تعویض نامنظم فرکانس کار
- تعویض نام معرف واحدها هم‌زمان با تعویض فرکانس
- آموزش کافی به کاروران در خصوص به‌کارگیری و رفع نواقص جزئی بی‌سیم‌ها
- رعایت سکوت و به گوش رادیویی در زمان‌های لازم

- ارسال کلیه پیام‌ها از طریق کد رمز حتی کوچک‌ترین مسائل و پیام‌ها
- برای مواقع عملیات تا حد ممکن کد رمزهای ضروری حفظ شود تا سرعت عمل بالا رود.
- استفاده از هر نوع بی‌سیم متناسب با مأموریت و شرایط زمین تا امکان هر گونه فعالیت دشمن روی ارتباطات ما کاهش یابد. مثلاً زمانی که ارتباطات نزدیک نیاز داریم از بی‌سیم برد بلند مانند ناصر خودرویی (VRC11110) و بی‌سیم ناصر کوله‌ای (PRC11 110) استفاده نکنیم.
- تا زمانی که لازم نیست از بی‌سیم استفاده نکنیم و از سایر لایه‌های ارتباطی امن‌تر مانند پیک و امر بر حداکثر استفاده را بنماییم.
- استفاده از تکنیک دورسازی: از آنجا که جنگال دشمن محل تشعشع امواج را شناسایی نموده و سپس موشک‌ها برای انهدام منبع به سمت آن هدایت می‌شوند در این روش برای جلوگیری از هدف قرارگرفتن کاربر بی‌سیم و نیروهای مجاور، پل بی‌سیم را جدا نموده روی استند مخصوص که دارای منبع تغذیه می‌باشد قرار می‌دهند سپس آن را تا فاصله مناسب که می‌توان تا ۵ کیلومتر این فاصله را از بی‌سیم داشت قرار می‌دهند و انجام فعالیت می‌نمایند. از جمله بی‌سیم‌هایی که این قابلیت را دارا است بی‌سیم ناصر می‌باشد
- استفاده از بی‌سیم‌های دارای رمزکننده
- استفاده از بی‌سیم‌های دارای پرش فرکانسی بالا (هاپینگ) مانند بی‌سیم فتاح که این بی‌سیم‌ها حدود ۵۰۰ پرش فرکانسی در یک ثانیه داشته و این امر باعث می‌شود حتی در صورت شناسایی و جهت‌یابی آنها ایجاد اختلال روی آنها دشوار باشد.
- از جمله سلاح‌هایی که ممکن است دشمن علیه ما استفاده کند بمب‌های الکترومغناطیس می‌باشد که باعث از بین رفتن تجهیزات الکترونیکی و مدارات برقی می‌شوند؛ لذا رعایت احتیاطات لازم در این مورد نیز لازم است از جمله اقداماتی که می‌توان انجام داد به مواردی

چون به‌همراه داشتن بی‌سیم یدکی، روشن نکردن بی‌سیم جزء در زمان لازم و حتی قرار ندادن باطری روی آن، تا زمان عدم نیازی توان اشاره نمود.

- استفاده از بی‌سیم‌های عملیاتی (موج کوتاه UHF)

- زمانی که ما شناسی بی‌سیم را می‌گیریم جنگال دشمن در مدت زمان بسیار اندکی می‌تواند ما را جهت‌یابی و مکان‌یابی نماید پس تا می‌توانیم باید از بی‌سیم استفاده ننماییم و در صورت استفاده زمان ارسال پیام را به حداقل برسانیم.

سیستم موقعیت‌یاب جهانی (GPS)

از جمله تجهیزاتی که در حال حاضر نیروهای نظامی به‌ویژه پیاده از آن استفاده زیادی جهت هدایت و ناوبری نیروها، هدایت آتش‌ها، موقعیت‌یابی و... می‌نمایند جی‌پی‌اس می‌باشد از مهم‌ترین علت‌های استفاده از این سیستم سرعت، دقت، جامع بودن و راحتی دسترسی به اطلاعات لازم از طریق آن می‌باشد. شاید بتوان گفت این سیستم تا حد زیادی جای نقشه و قطب‌نما را در نیروهای پیاده گرفته است که این خود باعث توجه کمتر نیروهای پیاده به اهمیت نقشه و قطب‌نما شده است. با وجود تمامی نکات مثبتی که جی‌پی‌اس دارد دارای نقاط ضعف قابل‌ملاحظه‌ای نیز است که در اینجا نقاط ضعف و ملاحظات آن در برابر جنگال دشمن به شرح زیر بیان می‌شود:

- قطع ارتباط آن از مرکز اصلی کنترل به‌صورت عمدی

- ایجاد خطای عمدی روی جی‌پی‌اس توسط دشمن به دو روش: ۱- حریف را در رسیدن به اطلاعات گمراه نموده و اطلاعات دقیق را در اختیار قرار ندهد ۲- به طور کاملاً هدفمند و هوشمندانه اطلاعاتی غلطی را که می‌خواهد به حریف بدهد (فریب).

- شناسایی موقعیت دقیق ما از طریق آن توسط دشمن

- ارسال اطلاعاتی که مادران ذخیره نموده و یا از آن استفاده نموده‌ایم به‌صورت خودکار و

مخفیانه برای مراکز کنترل

- خطا در اطلاعات آن در صورت کم رسیدن سیگنال به آن و یا دریافت سیگنال‌های منعکس شده و همچنین در زمان قرارگرفتن در میدان مغناطیسی (کشاوری ۵:۱۳۹۳) - امکان قطع ارتباط آن با ماهواره‌ها به وسیله سامانه‌های اختلال جی‌پی‌اس مانند سامانه‌های قائم و ستر که جنگال خودی در اختیار دارد در نقطه یا منطقه مورد هدف

- امکان قطع ارتباط آن با ماهواره‌ها به صورت منطقه‌ای و هوشمند توسط دشمن به وسیله سامانه‌های اختلال ماهواره‌ها مانند سامانه نجم که جنگال خودی دارد.

- امکان ایجاد خطای عمدی بر روی برند یا دستگاه خاص به صورت هوشمند

- هر دستگاه جی‌پی‌اس دارای ID مختص به خود می‌باشد که باتوجه به آن یک دستگاه وقتی در نقاط مختلف روشن می‌شود از طریق بررسی این کد می‌توان متوجه شد این دستگاه با این کد در چه مکان‌هایی استفاده شده و با کمی بررسی بیشتر از این طریق می‌توان به ماهیت کاربر آن نیز پی برد؛ یعنی ما ناخواسته به دشمن اعلام می‌کنیم که یک نیروی نظامی هستیم قبلاً چه مکان‌ها و عملیات بوده‌ایم و در حال حاضر در چه مکانی هستیم و بسیاری اطلاعات دیگر که تنها دشمن از این طریق به آن دست می‌یابد.

- دستیابی به اطلاعات دستگاه جی‌پی‌اس در اختیار ما توسط اقدامات جنگ الکترونیک دشمن

اقدامات قابل توجه در به کارگیری جی‌پی‌اس

از روشن کردن و استفاده از آن در مکان‌های نظامی و حساس اجتناب شود.

- در صورت ثبت مختصات نقطه‌ای حساس و مهم در آن برای منحصربه‌فرد نبودن آن نقطه تعدادی نقطه دیگر در آن زمان و مکانی که نقطه را ثبت نموده‌ایم ثبت نماییم.

- در انتخاب نام و سمبل نقاط و کروکی‌ها و... در دستگاه جی‌پی‌اس به گونه‌ای عمل کنیم

- که دشمن به راحتی از طریق آن‌ها نتواند به اهمیت اطلاعات ثبت شده پی ببرد.
- از جی‌پی‌اس که قبلاً در عملیات یا مکان و زمان خاصی استفاده کرده‌ایم در عملیات‌های مهم و حساس دیگر استفاده نکنیم.
- در صورت استفاده از جی‌پی‌اس در یک مکان جهت استفاده مثلاً ثبت نقطه از تعداد بیشتری جی‌پی‌اس استفاده شود و تعداد بیشتری نقطه علاوه بر نقاط اصلی هدف ثبت گردد.
- از جی‌پی‌اس‌های شرکت‌های مختلف استفاده نماییم؛ چون امکان اختلال بر روی نوع خاصی از دستگاه‌های جی‌پی‌اس وجود دارد.
- تا زمانی که لازم نیست منبع تغذیه روی آن قرار ندهیم.
- در زمانی که تنها قصد بهره‌برداری از اطلاعاتی را داریم که قبلاً در دستگاه ذخیره نموده‌ایم و نیاز به ارتباط دستگاه با ماهواره‌ها نمی‌باشد دستگاه را در حالت قطع ارتباط با ماهواره (GPS OFF) قرارداده سپس از آن استفاده کنیم. - مدت زمان استفاده از آن را تا حد ممکن کاهش دهیم.
- تا جایی که امکان استفاده از نقشه و قطب‌نما مهیا است از جی‌پی‌اس استفاده نکنیم.
- مهارت نیروها در نقشه‌خوانی و قطب‌نما به حدی رسانده شود که به راحتی بتوانند از آنها حداکثر استفاده را بنمایند و صرف راحتی بجای نقشه و قطب‌نما از جی‌پی‌اس استفاده نکنند.

دوربین‌های حرارتی و مادون قرمز

- شاید تصور بر این باشد که دوربین‌های مادون قرمز و حرارتی در برابر جنگال دشمن آسیب‌پذیر نبوده و مامی توانیم بدون محدودیت از آن‌ها استفاده نماییم؛ ولی متأسفانه این گونه نبوده و این تجهیزات نیز جزء تجهیزات آسیب‌پذیر در برابر جنگال هستند. برای فهمیدن علت آسیب‌پذیری این تجهیزات کافی است با نحوه عملکرد آنها به طور مختصر آشنا شوید. این

دوربین‌ها بسته به فناوری مورد استفاده خود به دو طریق کار می‌کنند:

۱- بهسازی تصویر (دوربین‌های مادون قرمز)

۲- تصویرسازی گرمایی (دوربین‌های حرارتی)

تجهیزات نوع اول یا بهسازی تصویر از روش جمع‌آوری و تقویت نورهای اندکی که از جسم متصاعد می‌شود و منابع نوری محدود موجود در محیط (ستاره‌ها و ماه) که با چشم غیرمسلح دیده نمی‌شوند استفاده می‌کند و دوربین‌های مادون قرمز نامیده می‌شوند. نوع دوم یا همان سامانه‌های تصویربردار حرارتی در ناحیه مادون قرمز میانی و بلند طیف الکترومغناطیسی کار می‌کنند. این سامانه‌ها از تابشی که از خود اجسام ساطع می‌گردد برای تصویربرداری بهره می‌برند. همان‌طور که می‌دانیم اجسام از خود امواج الکترومغناطیسی ساطع می‌کنند که طیف پیوسته‌ای را می‌پوشاند و طول موج پیک و میزان توان گسیلی آن به دمای جسم بستگی دارد؛ مثلاً می‌توانیم بگوییم که بدن جانداران بیشتر از اجسام سرد مانند درختان تشعشع دارند پس این دوربین‌ها با دریافت طیفی از انتشار الکترومغناطیسی اجسام کار تشخیص اجسام و ایجاد تصویری از آنها را اجرا می‌کنند.

سامانه‌های حرارتی برای ایجاد و بهبود قابلیت‌های عملیاتی نیروهای نظامی در رزم شبانه، امکان کشف و ردگیری اهدافی که از نظر دیداری از پنهان‌کاری و استتار خوبی استفاده کرده‌اند و همچنین ایجاد امکان ردگیری اهدافی که همواره منبع بزرگی برای تابش‌های حرارتی دارند ساخته شده‌اند. در نتیجه از آن جا که عملکرد این دوربین‌ها بر اساس امواج الکترومغناطیسی می‌باشد علت آسیب‌پذیری آن‌ها به راحتی توجیه می‌شود در زمان استفاده از این تجهیزات جنگال می‌تواند محل آن را کشف نماید و روی عملکرد آن‌ها تأثیر منفی بگذارد اگرچه امکان کشف آنها توسط سایر تجهیزات نیز امکان‌پذیر است. در نتیجه باید به

این مطلب توجه داشت که گرچه این دوربین‌ها امکان دیدن را در شب برای ما فراهم می‌کنند؛ ولی به همان اندازه هم امکان کشف شدن نیز توسط دشمن بالا می‌برند.

اقدامات لازم در به کارگیری دوربین‌های دید در شب

- باید در بکارگیری این تجهیزات دقت بیش‌تری نموده و بی‌پروا از آن‌ها استفاده ننماییم.
- تنها در زمان‌هایی که واقعاً نیاز داریم و گزینه دیگری نداریم از آن‌ها استفاده نماییم.
- زمان استفاده از آن‌ها را به حداقل برسانیم.
- تا زمانی که قصد استفاده از آن را نداریم آن را روشن ننماییم.
- هنگام به کارگیری از فریب استفاده نماییم؛ مثلاً استفاده هم‌زمان از آن‌ها در جاهای مختلف تا محل اصلی نیروها به راحتی کشف نشود.

موشک‌های ضد زره

از جمله سلاح‌های کاربردی که نقش مهمی در مقابله با دشمنان امروزی ما که به پیشرفته‌ترین تانک‌ها و خودروهای زرهی و تاکتیکی مجهز می‌باشند ایفا می‌کنند و یگان‌های پیاده و تکاور از آن بهره می‌برند موشک‌های ضد زره هستند که به تناسب تانک‌ها و خودروهای زرهی آن‌ها هم پیشرفت چشمگیری نموده‌اند. جنگال هم در این عرصه بیکار ننشسته و وارد عمل شده و در اصلی‌ترین بخش یعنی مقابله با این موشک‌ها به کمک تانک‌ها و خودروهای زرهی آمده امروزه بیشتر خودروهای پیشرفته دنیا جهت مقابله با موشک‌ها سیستم‌های پیشرفته‌ای دارند که سیستم جمینگ یکی از آن‌ها می‌باشد. این سیستم با ایجاد میدان مغناطیسی اطراف تانک و خودروهای زرهی باعث اختلال در سیستم رهگیری^۱ موشک شده و یا بانفوذ در سیستم هدایت موشک و فریب آن موشک را منحرف و سرنگون می‌نمایند. از جمله تانک‌های

^۱ Tracking

پیشرفته مجهز به این سیستم می‌توان به تانک مرکاوا ساخت رژیم اشغالگر اسرائیل اشاره نمود. باتوجه به مطالب بیان شده در اینجا نیز ما باید راهکاری پیدا نماییم تا بتوانیم با این بخش از جنگال دشمن مقابله نماییم. ازجمله اقدامات اساسی که ما می‌توانیم در مقابله با سیستم جمینگ تانک‌ها و خودروهای زرهی انجام دهیم به شرح زیر می‌باشد:

- استفاده از فریب به‌عنوان نمونه شلیک هم‌زمان دو موشک در یک راستا بافاصله زمانی بسیار اندک (۰,۵ ثانیه)

- استفاده از موشک‌هایی که سیستم ضد جمینگ دارند؛ مانند کورنت

- استفاده از موشک‌هایی که سیستم هدایت آن‌ها از قبضه بوده و قابل جمینگ نیستند.

استفاده از جنگال خودی جهت اختلال در سامانه‌های جنگال تجهیزات دشمن تا توانایی مقابله با موشک را نداشته باشند.

- استفاده از تک‌تیراندازها جهت هدف قراردادن رادارهای سیستم‌های جمینگ تجهیزات دشمن به‌منظور از کارانداختن و یا کاهش توانایی آنها جهت مقابله با موشک‌ها

گوشی همراه

هرچند گوشی همراه جزء تجهیزات یک نیروی نظامی محسوب نمی‌شود و حتی جزء وسایلی است که به‌همراه داشتن و استفاده از آن در بسیاری از موقعیت‌های زمانی و مکانی برای یک نظامی ممنوع می‌باشد؛ ولی متأسفانه از جمله تجهیزاتی است که هر یک از نیروهای ما در همه‌جا از جمله مراکز نظامی و عملیات‌ها به همراه دارند گوشی همراه است. از آن تأسف‌بارتر این است که به خطرات آن توجهی نمی‌کنند گوشی‌های همراه را می‌توان به دودسته کلی تقسیم‌بندی نمود: ۱- گوشی‌های غیروشمند ۲- گوشی‌های هوشمند هر دو نوع گوشی همراه در برابر جنگال آسیب‌پذیر می‌باشد. هرچند میزان آسیب‌پذیری آن‌ها متفاوت است و گوشی‌های غیروشمند آسیب‌پذیری کمتری دارند؛ ولی این امر استفاده از

آن‌ها را توجیه نمی‌کند. دشمن به وسیله اقداماتی که انجام می‌دهد می‌تواند از طریق شنود، سرقت اطلاعات، ردیابی و ردگیری و... گوشی همراه به اطلاعات ارزشمندی دست پیدا کند از جمله: پی‌بردن به ماهیت کاربر آن، محل تجمع نیروها و... نکات قابل توجه:

- عدم استفاده و به‌همراه داشتن گوشی همراه در پایگاه‌ها و مقرهای عملیاتی و مهم
- عدم استفاده و به‌همراه داشتن گوشی همراه در عملیات‌ها و مأموریت‌های حساس
- عدم ذخیره‌سازی اطلاعات نظامی در گوشی همراه
- عدم انتقال اطلاعات نظامی و مهم از طریق مکالمات به‌ویژه در مناطق عملیاتی و در مأموریت‌ها
- عدم انتقال اطلاعات نظامی در قالب صوت، عکس، فیلم و... از طریق گوشی همراه در بستر اینترنت و فضای مجازی
- استفاده از گوشی‌ها یا تبلت‌های عقیم‌سازی شده در صورت نیاز برای امورات نظامی که قابلیت استفاده از سیم‌کارت و اتصال به اینترنت را ندارند.
- از آن‌جا که گوشی‌های همراه قابلیت شنود محیطی دارند باید از ورود آن‌ها به جاهای حساس و جلسات جدا خودداری نموده و حتماً باید گوشی را خاموش کرده و باطری آن را برداشته و در محل مخصوص و بافاصله نگهداری شود.

راهکارهای مهم درباره این مبحث:

- ۱- توسعه تجهیزاتی و پرسنلی واحدهای جنگال در یگان‌ها: امروزه واحدهای جنگال در یگان‌ها فعال هستند؛ ولی به دلایلی چون کمبود پرسنل متخصص و نبود تجهیزات کافی قادر به تأمین نیاز یگان خود نمی‌باشند و معمولاً به صورت متمرکز و تعاملی با سایر واحدهای جنگال در سراسر کشور ایفای مأموریت می‌نمایند که اگر از لحاظ پرسنل و تجهیزاتی توسعه

یابند بهتر و بیشتر قادر به تأمین نیاز یگان خود خواهند بود.

۲- باید از جنگال به عنوان یکی از عناصر اصلی یگان‌ها در مأموریت‌های یگان استفاده شود. در این صورت توانمندی‌ها و کارایی‌های آن بیشتر برای فرماندهان و نیروها روشن خواهد شد.

۳- انجام مانورهایی که در آن جنگال خودی نقش جنگال دشمن را ایفا می‌نماید به نحوی که فرماندهان نیروها را در شرایطی مشابه اقدام جنگال دشمن قراردادده مانند اختلال و یا قطع ارتباطات و سامانه‌های موقعیت‌یابی و ناوبری تا فرماندهان و نیروها با قرارگرفتن در این شرایط شبیه‌سازی شده بتوانند توانایی خود را در برابر جنگال دشمن محک زده نقاط ضعف خود را یافته و آن را از بین ببرند.

نتیجه‌گیری

باتوجه به وسعت جنگ الکترونیک در نبردهای امروزی و آسیب‌پذیری بالای نیروهای پیاده و تکاور که در نوک پیکان میدان نبرد هستند باید تجهیزات و سلاح‌های آسیب‌پذیر این یگان‌ها در برابر جنگال دشمن متناسب با تهدیدات جنگال دشمن طراحی و ساخته شده و آموزش‌های لازم و مستمر جنگ الکترونیک باتوجه به پیشرفت‌ها و تغییراتی که در عملکرد جنگال دشمن شکل می‌گیرد برای یگان‌های پیاده تکاور لحاظ گردد. در یگان‌های پیاده تکاور برای جنگال اهمیت ویژه قائل شده و جهت تأمین کادر تخصصی و تجهیزات تخصصی و به‌روز جنگال فرماندهان یگان حداکثر تلاش خود را بنمایند. از آن جا که امروزه دشمن در تمامی عملیات‌های خود از جنگال بهره می‌برد شرط لازم برای موفقیت آشنایی نیروها با جنگال و داشتن جنگال قوی و تجهیزاتی است که کمترین آسیب‌پذیری را در مقابل جنگال دشمن داشته باشد. حال باید دنبال این پاسخ باشیم که چرا در حال حاضر به واحدهای جنگال در یگان‌ها توجه نمی‌شود و اینکه واحدهای جنگال با تجهیزاتی که در حال حاضر دارند چه میزان از نیاز یگان‌ها را می‌توانند برآورده سازند؟

منابع

- امیر مصلح، (۱۳۸۸). تاکتیک‌ها و تکنیک‌های اختلال جنگ الکترونیک، معاونت آموزش نرسا
- دستورالعمل جنگ الکترونیک (۱۳۸۶). چاپ اول، صایران، شرکت صنایع دفاع الکترونیک
- محمدی، حسین (۱۳۸۷). جنگ الکترونیک در نبرد نامتقارن، معاونت آموزش نرسا
- کشاورز، حسن (۱۳۹۳)، موقعیت یاب ماهواره‌ای GPS map 62s، مرکز تحقیقات و فناوری آموزشی نرسا
- طلعتی، سعید؛ اصلی نژاد، مهدی (۱۳۹۶). اصول جنگ الکترونیک، چاپ اول، انتشارات پشتیبان
- کالوندی، سیدمحمدرضا (۱۳۷۴). «جنگ الکترونیک»، پایان‌نامه مقطع کارشناسی رشته الکترونیک دانشگاه آزاد واحد سیستان و بلوچستان
- درویشی، فرهاد (۱۳۸۵). «جنگ آینده»، ماهیت ابعاد و مسائل، فصلنامه مطالعات دفاعی و امنیتی، سال هشتم، شماره ۲۱، زمستان
- اندیشگاه شریف (۱۳۸۸). پارادایم‌های حاکم بر جنگ‌های آینده، تهران: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده پژوهی علوم و فناوری دفاعی