حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی حریفان با رویکرد پدافند غیرعامل

تاریخ دریافت: ۱۳۹۳/۱۱/۲۰
تاریخ تأیید: ۱۳۹۳/۱۲/۲۴

محسن مرادیان[۱]
حمیدرضا سوری[۲]
مصطفی دهقانی[۳]

چکیده

شبکه‌ها و تجهیزات ارتباطی از زیرساخت‌های اصلی سامانه‌های فرماندهی و واپایش میدان نبرد هستند که همواره به‌عنوان اهدافی برای اقدامات جنگ الکترونیک دشمن به‌شمار می‌روند. اقدامات جنگ الکترونیک دشمن علیه سامانه‌های ارتباطی در دو بخش پشتیبانی الکترونیکی و تهاجم الکترونیکی انجام می‌شوند. مقاله حاضر باهدف «شناخت و چگونگی محافظت سامانه‌های ارتباطی در برابر اقدامات پشتیبانی الکترونیکی حریفان با رویکرد پدافند غیرعامل» با متغیر مستقل حفاظت ارتباطات رادیویی و متغیر وابسته اقدامات پشتیبانی الکترونیکی حریفان به روش توصیفی– تحلیلی انجام شده است. این مقاله با این فرضیه که؛ «محافظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی حریفان، با به‌کارگیری روش‌های فعال و غیرفعال انجام می‌شود» به‌دنبال پاسخ‌گویی به این سؤال اساسی است که «چگونه می‌توان سامانه های ارتباطی رادیویی را در برابر اقدامات پشتیبانی الکترونیکی حریفان محافظت نمود؟». ابزار گردآوری اطلاعات پرسشنامه ساختهٔ پژوهشگر و مصاحبه با نخبگان حوزه جنگ الکترونیک و ارتباطات آجا است که اعتبار آن با استفاده از روش دلفی تأیید و پایایی آن با استفاده از آزمون ضریب آلفای کرونباخ ۹۱/۸۳ درصد تعیین شده است. تحلیل داده‌ها با روش توصیفی و استنباطی، آزمون فرضیه با روش t تک نمونه‌ای و اولویت‌بندی مؤلفه‌ها با ابزار فریدمن انجام شده است. براساس نتایج به‌دست آمده، اقدامات محافظت الکترونیکی سامانه‌های ارتباطی به دو روش فعال و غیرفعال انجام می‌شود که می‌بایست در مراحل طراحی، تولید و بهره‌برداری عملیاتی سامانه‌ها و پس از آن درنظر گرفته شود.

کلید واژه‌ها: *ارتباطات رادیویی، جنگ الکترونیک، پشتیبانی الکترونیکی، پدافند غیرعامل.*

۱- استادیار امنیت ملی دانشگاه عالی دفاع ملی (mohsenmoradian@hotmail.com)
۲- کارشناسی ارشد اطلاعات و حفاظت اطلاعات دانشکده علوم و فنون فارابی (H_r_souri@yahoo.com)
۳- کارشناسی ارشد پدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی(نویسنده مسئول) (md.1000@ chmail.ir)

مقدمه

فناوری اطلاعات و ارتباطات محرک اصلی در انقلاب اطلاعاتی و درنتیجه عامل اصلی تغییر ماهیت و شیوه‌وشگردهای نبردهای امروزی است. فرآیند جمع‌آوری، پردازش و توزیع صحیح و به‌موقع اطلاعات که از عوامل مهم دستیابی به پیروزی در این نبردها است با بهره‌گیری از ارتباطات امن، پایدار، برخط[1] و بی‌درنگ[2] تأمین می‌شود. از طرف دیگر با رشد و گسترش فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یادشده گسترده‌تر و پیچیده‌تر می‌گردد. ازاین‌رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهم‌ترین هدف‌های گسترش فناوری اطلاعاتی و ارتباطی به‌شمار می‌آید.

افزایش اهمیت اطلاعات و ارتباطات در جنگ‌های نوین، طرف‌های درگیر در میدان نبرد را بر آن داشته است تا با انجام اقدامات جنگ الکترونیک، با استفاده از سامانه‌های پشتیبانی الکترونیکی نسبت به جمع‌آوری اطلاعات از سامانه‌های ارتباطی طرف مقابل و با بهره‌گیری از سامانه های تهاجم الکترونیکی نسبت به مختل کردن و ممانعت از جریان صحیح و دقیق اطلاعات در سامانه‌های مدیریتی و فرماندهی حریف اقدام نمایند. بر این اساس محافظت از سامانه‌های ارتباطی میدان نبرد در مقابل اقدامات جنگ الکترونیک دشمنان، به‌منظور دستیابی به برتری اطلاعاتی و کسب پیروزی بر حریفان از بایدهای جنگ‌های نوین به‌شمار می‌آید. از سوی دیگر عملکرد بیشتر سامانه‌های اطلاعاتی و ارتباطی که شالوده و زیرساخت چرخه فرماندهی و واپایش به‌شمار می‌روند؛ براساس طیف الکترومغناطیس است که به‌همین دلیل در برابر اقدامات جنگ الکترونیک دشمن آسیب‌پذیر هستند. این مقاله چگونگی محافظت سامانه‌های ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی دشمن را بررسی و ارائه می‌کند.

بیان مسئله

ارتباطات از ابتدایی‌ترین شکل آن تا پیشرفته‌ترین نوع و ساختار، همواره در نبردها نقشی حیاتی داشته‌اند که امروزه این نقش بسیار پررنگ‌تر از گذشته خود را در مؤلفه‌های اصلی جنگ‌های امروزی و ازجمله سامانه‌های فرماندهی و واپایش به‌خوبی نشان داده است. هماهنگی و مدیریت عملیات نظامی یکپارچه که از شاخصه‌های نبردهای نوین به‌شمار می‌آید، بدون شبکه‌های ارتباطی امکان‌پذیر نیست. ارتباطات موجود در میدان عملیات با استفاده از سامانه‌ها

1. On Line
2. Real Time

و تجهیزات بی‌سیم و باسیم برقرار می‌گردد. این سامانه‌ها علاوه بر برتری‌ها و فرصت‌ها، دارای آسیب‌پذیری و تهدیدهای خاص خود نیز هستند. شاید بتوان گفت بیش‌ترین تهدید متوجه سامانه‌های بی‌سیم و ارتباطات رادیویی است. ازآنجاکه سیگنال‌های[1] این نوع ارتباطات در فضا منتشر می‌شوند، عملاً واپایش کامل بر آن امکان‌پذیر نبوده و فرصتی را در اختیار حریفان (که غالباً صاحبان فناوری جنگ الکترونیک هستند) قرار می‌دهد که ضمن بهره‌برداری از آن، اقدامات تهاجم الکترونیک خود را متوجه این نوع ارتباط نمایند. در حوزه جنگ الکترونیک اقدامات پشتیبانی الکترونیکی (کشف، شناسایی، شنود، تعیین موقعیت و تحلیل ارسال‌ودریافت‌ها) و تهاجم الکترونیکی (فریب، اختلال و انهدام) علیه سامانه‌ها و شبکه‌های ارتباطی انجام می‌شود و ویژگی‌های آن سامانه‌ها همچون اطمینان‌پذیری، امنیت، درستی و صحت اطلاعات، دسترس‌پذیری، تصدیق هویت و... را تهدید می‌کنند (Roger J. Sutton, 2002: 4). با توجه به جایگاه و نقش تجهیزات و شبکه‌های ارتباطی در سامانه فرماندهی و واپایش میدان نبرد، برای حفظ ابتکار عمل در هرگونه درگیری در آینده و بهره‌برداری از برتری‌های سامانه‌های ارتباطی و اطلاعاتی در میدان‌های نبرد، بایستی از سامانه‌های ارتباطی خودی در برابر اقدامات پشتیبانی الکترونیکی و تهاجم الکترونیکی دشمن محافظت نمود. به نظر می‌رسد در حال حاضر به دلایل مختلف به همهٔ ابعاد تهدیدها و آسیب‌پذیری‌های ارتباطات رادیویی در حوزه جنگ الکترونیک توجه نمی‌شود و در نتیجه حفاظت از سامانه‌های ارتباطی به‌عنوان چالش اصلی نیروهای مسلح در برابر اقدامات حریفان در این حوزه است.

اهمیت و ضرورت

مدیریت مؤثر در میدان نبرد علاوه بر جمع‌آوری، تحلیل اطلاعات و تصمیم‌گیری به ارتباط بین گره‌های عملیاتی وابسته است. ارتباطات امن، پایدار و برخط مقدمه ایجاد هماهنگی بین عناصر میدان نبرد به‌شمار می‌رود. حجم گسترده‌ای از ارتباطات در این میدان‌ها به‌صورت رادیویی و با بهره‌گیری از طیف الکترومغناطیس انجام می‌شود و به‌همین دلیل در برابر اقدامات جنگ الکترونیک حریفان آسیب‌پذیر هستند. اگر سامانه‌های ارتباطی نابود شوند، واپایش فرمانده بر میدان جنگ کاهش یابد، یا این سامانه‌ها فریب داده شوند، فرمانده و ستادش نمی‌توانند جنگ را به‌طور مناسب پیش ببرند. نبود ارتباطات در میدان نبرد نوین مانند آن است که فرمانده توانایی دیدن، شنیدن و گفتن خود را از دست داده است (Michael Ryan and Michael Frater, 2001: 14).

1. Signals

مقام معظم رهبری تاریخ ۱۳۸۸/۱۱/۳۰ در مراسم پیوستن ناوشکن جماران به ناوگان نیروی دریایی ارتش جمهوری اسلامی ایران دربارهٔ اهمیت جنگ الکترونیک و دفاع الکترونیک فرمودند: «یک مسئله هم مسئله جنگ الکترونیک است. من بارها در طی سال‌ها هم در دیدار با نیروی دریایی، هم در دیدار با نیروی هوایی، روی مسئله جنگ الکترونیک تأکید کرده‌ام، باز هم تأکید می‌کنم. دشمنان شما بر روی توانایی‌های الکترونیکی در زمینه سلاح‌های جنگی متمرکزند و سال‌ها هم هست که دارند کار می‌کنند. دفاع الکترونیکی برای ما خیلی مهم است. روی مسائل الکترونیک کار کنید». معظم له دربارهٔ اهمیت محافظت از ارتباطات در رزمایش بزرگ پیروان ولایت فرمودند: «حتی یک یگان شما هم نباید در منطقه احساس تنهایی کند، به هر کیفیتی هست باید رابطه (ارتباط) را با او برقرار کنید.» (مجموعه بیانات رهبر معظم انقلاب ۸۸/۱۱/۳۰)

نبود شناخت کامل دربارهٔ تهدیدها و آسیب‌های این حوزه موجب کاستی در راهبردها، سیاست‌ها و شیوه‌نامه‌های حفاظت از ارتباطات رادیویی و در نتیجه کاهش اقدامات عملیاتی در این حوزه و فرصت‌سازی برای بهره‌برداری حریفان از این حوزه‌ی مهم و راهبردی خواهد بود. همچنین سامانه مدیریت اطلاعات (جمع‌آوری، تجزیه‌وتحلیل و توزیع) کارایی خود را از دست داده و درنتیجه اشراف اطلاعاتی که لازمه هر نبرد موفقی است، میسر نخواهد شد.

هدف، سؤال و فرضیه

این مقاله با هدف «شناخت و چگونگی محافظت سامانه‌های ارتباطی در برابر اقدامات پشتیبانی الکترونیکی حریفان با رویکرد پدافند غیرعامل» به‌دنبال پاسخ‌گویی به این سؤال اساسی است که «چگونه می‌توان سامانه‌های ارتباطی رادیویی را در برابر اقدامات پشتیبانی الکترونیکی حریفان محافظت نمود؟». فرضیه مقاله این است که «حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی حریفان، با به‌کارگیری روش‌های فعال و غیرفعال انجام می‌شود.» فرضیه فرعی مقاله نیز این است که حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات فعال شامل رمزنگاری با الگوریتم بومی، فناوری‌های با احتمال ره‌گیری پایین و کدینگ و قراردادهای ارتباطی بومی انجام می‌شود.

فرضیه فرعی بعدی نیز این است که حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات غیرفعال شامل مدیریت توان، مدیریت طیف و بسامد و طراحی هوشمند شبکه‌های ارتباطی؛ انجام می‌شود.

پیشینه

۱. خردمند، محمد (۱۳۸۸) در پایان‌نامه کارشناسی ارشد خود با موضوع «به‌کارگیری عوامل مؤثر سامانه ارتباطی فرکانس بسیار بالا[1] گردان‌های پیاده نزاجا در مقابله با نیروهای فرامنطقه‌ای» به این نتیجه رسیده که، استفاده از آنتن‌های همه جهته و جهتی در سامانه‌های ارتباطی بسامد بسیار بالا، تقویت امنیت ارتباطات با استفاده از رمزکننده‌های برخط بومی و سوار کردن سامانه‌های ارتباطی بر خودرو و نفر در مقابله با نیروهای فرا منطقه‌ای مؤثر است.

۲. مقاله‌ای با عنوان «ایمن‌سازی مخابرات رادیویی در محیط جنگ الکترونیک با بهره‌گیری از روش ارسال جهتی» توسط فاطمی مفرد و میار در ششمین همایش ملی جنگ الکترونیک ایران در مهرماه ۱۳۹۲ ارائه شده که براساس نتایج آن، در روش ارسال جهتی با محدود کردن فضای ارسال و دریافت در راستای واحدهای گیرنده و فرستنده، ارتباط واقعی ایمن‌تر می‌شود و از انتشار ناخواسته سیگنال در همه جهت‌ها جلوگیری به‌عمل می‌آید و دشمن در دریافت، شنود و اختلال سیگنال با مشکل مواجه می‌شود.

مفاهیم و مبانی نظری

۱.ارتباطات رادیویی و عوامل مؤثر بر آن: هدف سامانه‌های ارتباطی، انتقال اطلاعات از نقطه‌ای به نقطه دیگر است. یک سامانه ارتباطی از سه بخش فرستنده، کانال انتقال (کانال ارتباطی) و گیرنده تشکیل شده است. کانال ارتباطی به دو نوع باسیم (خطوط زوج‌سیم، موج‌بر[2]، فیبرنوری و ...) و بی‌سیم با بهره‌گیری از طیف الکترومغناطیسی تقسیم می‌شود (پالی جوزف، ۱۳۷۴: ۱۶). نوع دوم به ارتباط رادیویی معروف است.

برای طراحی و پیاده‌سازی شبکه‌های ارتباطی سه عامل اصلی انتشار رادیویی بین فرستنده و گیرنده، عوامل محیطی تأثیرگذار بر انتشار رادیویی و فرستنده‌ها و گیرنده‌های رادیویی مورد توجه قرار می‌گیرند (Adrian Graham, 2011: 191).

۱-۱ انتشار رادیویی: سرعت انتشار امواج الکترومغناطیس در فضا برابر سرعت انتشار نور و تقریباً معادل ۳×۱۰^{۸} متر بر ثانیه است. امواج الکترومغناطیسی بازه گسترده‌ای از بسامد را شامل می‌شوند و همهٔ امواج رادیویی، فروسرخ، نور مرئی، فرابنفش، اشعهٔ ایکس و گاما را دربر می‌گیرند (ابراهیمی و همکاران، ۱۳۹۰: ۴۷).

۱-۲ کاربردهای امواج رادیویی: از امواج رادیویی برای انتقال انواع مختلف اطلاعات صوتی، تصویری، داده[3]، واپایش و ناوبری در سامانه‌های ارتباطات زمینی[4]، دریایی[1] و هوایی[2] برای ارائه

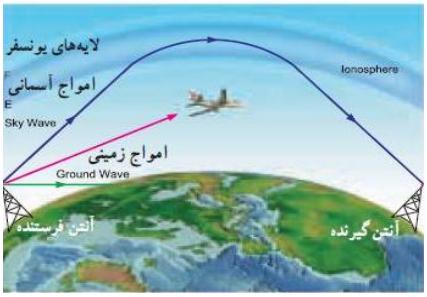
1. Very High Frequency (VHF)
2. Waveguide
3. Data
4. Land Radio Communications

خدمات گوناگون از جمله ارتباطات متحرک زمینی، دریایی و هوایی، ارتباط‌های ثابت نقطه‌به‌نقطه، ارتباط‌های ماهواره‌ای، سامانه‌های پخش صوتی و تصویری همگانی، سامانه‌های کمک ناوبری و تعیین موقعیت رادیویی، رادیو آماتور و کیهان‌شناسی و پژوهش‌های فضایی بهره گرفته می‌شود (قاسمی، ۱۳۸۵: ۲۳۴).

۱-۳ مسیرهای ارتباط رادیویی: مسیرهای مختلفی برای ارتباط بین فرستنده و گیرنده رادیویی وجود دارد. این مسیرها به عواملی چون بسامد، نوع آنتن و ارتفاع آن، شرایط جوی و عوارض زمین بستگی دارد (Martin H. Barringer, 2013: 191).

عمده‌ترین مسیرهای ارتباطی برابر شکل شماره ۱ عبارت‌اند از:

- موج زمینی[3]: موج زمینی موجی است که مسیر حرکتش در سطح زمین است و انحنای زمین را طی می‌کنند.
- موج در امتداد دید (خط دید مستقیم)[4]: انتشار موج فضایی به انتشار در امتداد دید نیز معروف است چون برای برقراری ارتباط باید فرستنده و گیرنده در دید مستقیم یکدیگر قرار بگیرند.
- موج آسمانی[5]: موج آسمانی به موجی گفته می‌شود که در آن موج رادیویی منتشرشده در فضا بعد از برخورد با لایه‌های یونیزه جو (یونسفر) دوباره به طرف زمین منحرف می‌گردد (قاسمی، ۱۳۸۵: ۱۰).



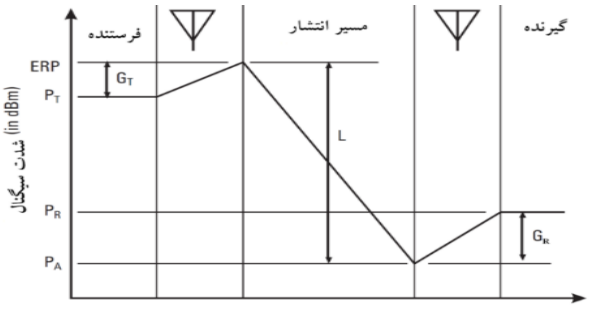
شکل ۱: مسیرهای مختلف انتشار امواج رادیویی (قاسمی، ۱۳۸۵: ۱۰).

لایه‌های جو زمین: در جو زمین ترکیبی از گازهای گوناگونی ازجمله گازهای اکسیژن، ازت، گازهای کربنیک و بی‌اثر همچون رطوبت وجود دارد که بر مقدار، ترکیب و توزیع آن‌ها عوامل مختلفی مانند اثر خورشید، فصل‌های مختلف، ساعت و ... اثرگذار است. جو زمین برحسب

1. Maritime Radio Communications
2. Aeronautical Radio Communications
3. Ground Wave
4. Line Of Sight (L.O.S)
5. Sky Wave

چگونگی دما، اختلاف چگالی، تغییرهای فشار، تداخل گازها و ویژگی‌های الکتریکی به لایه‌های تروپوسفر[1]، استراتسفر[2]، مزوسفر[3]، یونسفر[4] و اگزوسفر[5] تقسیم شده است (ابراهیمی و همکاران، ۱۳۹۰: ۲۲). در بین لایه‌های جو، دو لایه تروپوسفر و یونسفر در انتشار امواج رادیویی مؤثرتر هستند (Richard S.Deakin, 2010: 294).

عوامل محیطی تأثیرگذار بر انتشار رادیویی: در ارتباطات، فرستنده و گیرنده در مکان‌های متفاوتی قرار دارند. هدف همهٔ انواع سامانه‌های ارتباطی، انتقال اطلاعات از نقطه‌ای به نقطه دیگر است. این ارتباط با استفاده از فرستنده، گیرنده، آنتن‌های ارسال و دریافت و هر پدیده‌ای که بین این دو آنتن برای سیگنال اتفاق می‌افتد، برقرار می‌شود. عوامل مؤثر بر این ارتباط عبارت‌اند از: توان خروجی فرستنده، بهره آنتن فرستنده، اتلاف انتشار در مسیر بین آنتن‌های ارسال و دریافت، بهره آنتن دریافت‌کننده و سامانه گیرنده (دیوید آدامی، ۱۳۹۲: ۲۲۱-۲۲۶). تأثیر این عوامل در شکل شماره ۲ نشان داده شده است.



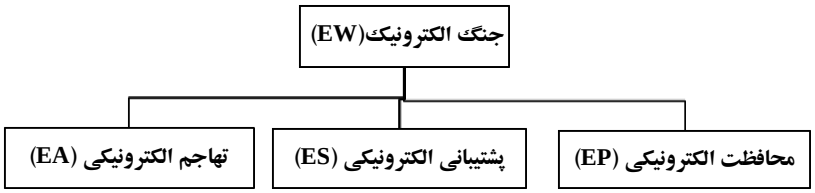
شکل شماره ۲: فرایند پیوند ارتباطی (همان).

بررسی آسیب‌پذیری‌ها و تهدیدهای ارتباطات رادیویی در حوزه جنگ الکترونیک

تعریف جنگ الکترونیک: جنگ الکترونیک، هنر و علم جلوگیری از بهره‌مندی دشمن از طیف الکترومغناطیس و همچنین محافظت از آن برای استفاده نیروهای خودی است (David Adamy, 2011: 4). جنگ الکترونیک سلسله اعمالی است که از انرژی نهفته در طیف الکترومغناطیس برای شناسایی، بهره‌برداری اطلاعاتی، کاهش یا جلوگیری از استفاده مؤثر دشمن از طیف الکترومغناطیس خود و تداوم استفاده نیروهای خودی از طیف صورت می‌گیرد (سنگرگیر، مراد، جواهری، علیرضا، ۱۳۹۱: ۳۳۵). سه بخش عمده جنگ الکترونیک عبارت است از:

1. Troposphere
2. Stratosphere
3. Mesosphere
4. Ionosphere
5. Exosphere

پشتیبانی الکترونیکی[1]، تهاجم الکترونیکی[2] و محافظت الکترونیکی[3] (شکل شمارهٔ ۳). با پشتیبانی الکترونیکی فرماندهان می‌توانند برآوردی دقیق از صحنه نبرد، تهدید و فرصت‌های پیشرو داشته باشند. تهاجم الکترونیکی استفاده دشمن از طیف الکترومغناطیس را محدود می‌کند. محافظت الکترونیکی استفاده نیروهای خودی از طیف الکترومغناطیس را حمایت و محافظت می‌نماید (نیروی هوایی آمریکا، ۱۳۹۰: ۳۱ و ۳۲).



شکل شماره ۳: بخش‌های اصلی جنگ الکترونیک (همان)

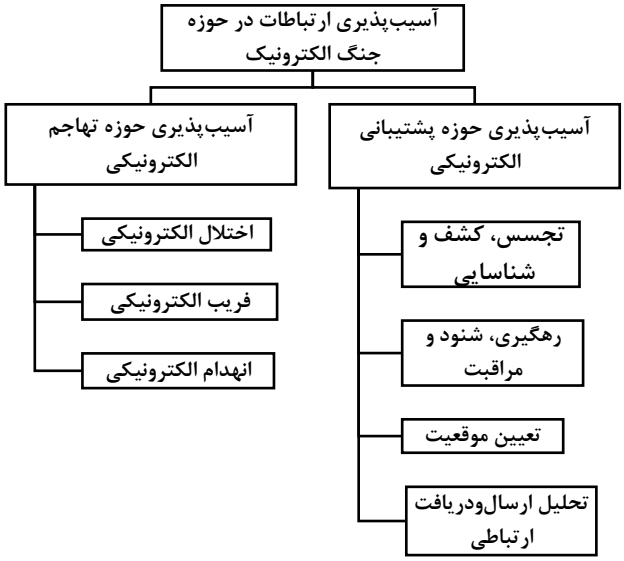
هدف‌های اصلی جنگ الکترونیک: جنگ الکترونیک سه هدف اصلی دارد که به شرح زیر است:

- دست‌یابی به توان جستجو، ره‌گیری، آشکارسازی، شناسایی، شنود و نفوذ در سامانه‌ها، شبکه‌ها و فضای الکترومغناطیس دشمن به‌منظور جمع‌آوری اطلاعات سیگنالی.
- دست‌یابی به توان اجرای اقدامات آفندی دربرابر سامانه‌ها، شبکه‌ها و طیف الکترومغناطیس دشمن (اختلال، فریب و انهدام) به‌منظور کاهش کارایی.
- دست‌یابی به توان محافظت از فضای طیف الکترومغناطیس خودی در برابر نفوذ و اقدامات آفندی دشمن (واحدی، ۱۳۹۰: ۱۹).

آسیب‌پذیری‌های ارتباط‌های رادیویی در حوزه جنگ الکترونیک

سامانه‌ها و تجهیزات ارتباطی و اطلاعاتی زیرساخت اصلی سامانه‌های فرماندهی و واپایش میدان نبرد هستند و وابستگی شدیدی به امواج الکترومغناطیس و به‌کارگیری مدارهای الکترونیکی دارند؛ بنابراین در جنگ‌های نوین، ضربه زدن به این سامانه‌ها با استفاده از فضای امواج الکترومغناطیسی در اولویت نخست قرار دارد و قبل از هرگونه اقدام نظامی، جنگ الکترونیک اولین قدم در صحنه نبرد خواهد بود. آسیب‌پذیری‌های ارتباطات در حوزه جنگ الکترونیک در دو بخش پشتیبانی الکترونیکی و تهاجم الکترونیکی تقسیم می‌شود که اقدامات هر بخش در شکل شماره ۴ نشان داده شده است. در این مقاله آسیب‌پذیری بخش پشتیبانی الکترونیکی و چگونگی مقابله با آن‌ها بررسی می‌شود.

1. Electronic Support (ES)
2. Electronic Attack (EA)
3. Electronic Protection (EP)



شکل شمارهٔ ۴: آسیب‌پذیری‌های ارتباطات رادیویی در حوزه جنگ الکترونیک.

آسیب‌پذیری‌های ارتباطات رادیویی در حوزه پشتیبانی الکترونیکی: اصلی‌ترین مسؤلیت‌های پشتیبانی جنگ الکترونیک جمع‌آوری اطلاعات و ایجاد اطلاعات عملیاتی[1]، هدایت برای انجام تهاجم الکترونیکی و دادن رهنمود دربارهٔ منابع مراقبت و ره‌گیری هدف است. جستجو، ره‌گیری، موقعیت‌یابی و تحلیل ارسال‌ودریافت سیگنال عمده‌ترین فعالیت‌های پشتیبانی الکترونیکی هستند که علیه سامانه‌های ارتباطی انجام می‌شود. اطلاعاتی که از فرآیندهای پشتیبانی الکترونیکی به‌دست می‌آید برای تشخیص و ترسیم آرایش الکترونیکی میدان نبرد و پی بردن به نیت‌های فرمانده دشمن استفاده می‌شود.

جستجو، کشف و شناسایی: در این مرحله طیف الکترومغناطیس پایش شده و سیگنال‌های فعال کشف، بررسی و شناسایی می‌شوند. شناسایی در دو بخش مشخصات فنی سیگنال (بسامد، دامنه سیگنال و...) و مشخصات عملیاتی (مشخصات هویت کاربر سیگنال) انجام و نتیجه در پایگاه داده ذخیره می‌شود. براساس این اطلاعات، هدف‌های موردنظر به جایگاه‌های ره‌گیری، موقعیت‌یاب و ... واگذار می‌گردند.

ره‌گیری، شنود و مراقبت: در این مرحله فعالیت سیگنال هدف همیشه واپایش می‌شود و محتوای سیگنال ارتباطی دریافت و ضبط می‌شود.

1. Operational Intelligence

موقعیت‌یابی: در این مرحله با کمک اطلاعات به‌دست آمده از فرآیندهای سمت‌یابی[1] که براساس پردازش‌های مرحلهٔ جستجو انجام می‌شود، موقعیت جغرافیایی فرستنده‌های دشمن تعیین می‌گردد. این کار با روش‌های مختلفی انجام می‌شود که یکی از مفیدترین و نیز ساده‌ترین روش‌ها روش مثلث‌بندی[2] است (شکل شماره ۵).

شکل شماره ۵: مکان‌یابی یک فرستنده فرضی با استفاده از روش مثلث‌بندی.

تحلیل ارسال‌ودریافت: تحلیل ارسال‌ودریافت سیگنال درواقع فرآیند ره‌گیری و بررسی آماری فعالیت‌های سیگنالی برای دست‌یابی به اطلاعات از الگوهای تبادل اطلاعات، در شبکه ارتباطی است. این کار را حتی در حالتی که پیام‌ها به‌صورت رمز هستند نیز می‌توان انجام داد. تحلیل ارسال‌ودریافت در زمینهٔ جمع‌آوری اطلاعات و حفاظت از اطلاعات ارتباطی و رایانه‌ای کاربرد دارد. با بررسی ارتباطات هر فرستنده با دیگر گیرنده و فرستنده‌ها می‌توان جریان اطلاعات میدان نبرد را مشخص کرد (Terry, I. 2003). جمع‌آوری سنتی اطلاعات ارتباطی با ره‌گیری و شنود ارتباطات، بهره‌برداری از ارتباطات دشمن و پایش محتوای گفتگوها انجام می‌شود اما تحلیل اطلاعات فراداده‌ها نه بر پایه محتوای پیام‌ها بلکه براساس داده‌های ارتباطی فنی به جمع‌آوری اطلاعات می‌پردازد. اطلاعات ارتباطی غیرمحتوایی، بیشتر برای دست‌یابی به اطلاعات کمّی در مورد کاربری یک فرستنده خاص همانند مکان، حجم فعالیت، مسیر حرکت و ... استفاده می‌شود (دهقانی و همکاران، ۱۳۹۰: ۳).

محافظت ارتباطات رادیویی با رویکرد پدافند غیرعامل: در زمان صلح، ضرورت آمادگی برای جنگ از خود جنگ مهم‌تر است. با گذشت زمان و با پیشرفت علوم و فناوری، روش‌های گوناگون، هوشمندانه و هدفمندی برای جنگ و دفاع در عرصه‌های نظامی به‌کار گرفته شده است. نکته دارای اهمیت درباره نقش فناوری در جنگ و دفاع این است که فناوری و به‌ویژه فناوری‌های

1. Direction Finding (DF)
2. Triangulation

اطلاعات و ارتباطات و گسترش زیرساخت‌ها و شبکه و استفاده از آن‌ها برای همه فراهم شده است ولی حوزه‌های امنیت و دفاع در انحصار دولت‌های صاحب فناوری است (جلالی فراهانی، ۱۳۹۰: ۲۳). براساس سیاست‌های کلی نظام دربارهٔ پدافند غیرعامل مصوب مجمع تشخیص مصلحت نظام، پدافند غیرعامل عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در برابر تهدیدها و اقدام‌های نظامی دشمن می‌شود (اسکندری، ۱۳۸۸: ۳۲). محافظت الکترونیکی بخش مهم و جدایی‌ناپذیر عملیات پدافندیِ جنگ الکترونیک است که در آن انرژی نهفته در طیف الکترومغناطیس خودی با دقّت و شدّت کامل در برابر جنگ الکترونیک دشمن حفاظت می‌شود. سامانه‌های ارتباطی و راداری خودی، هدف عمده و آسیب‌پذیرِ حملات الکترونیکی دشمن به‌شمار می‌آیند. در فرآیند دفاع الکترونیکی با استفاده از روش‌های گوناگون که در طراحی مدارهای الکترونیکی به‌کار رفته است، از پدافند غیرعامل نیز استفاده می‌شود (سنگرگیر و جواهری، ۱۳۹۱: ۳۳۱). محافظت الکترونیکی شامل انجام اقداماتی برای مقابله با تأثیرگذاری تهاجم الکترونیکی و پشتیبانی الکترونیکی دشمن بر تجهیزات الکترونیکی خودی است و از جنبه‌ای طرف مقابل تهاجم الکترونیکی و پشتیبانی الکترونیکی است. اقدامات محافظت الکترونیکی به دو بخش فعال و غیرفعال تقسیم می‌شوند. اقدامات فعال مانند رمزنگاری، مدولاسیون‌های احتمال شنود پایین و اخلال پوششی؛ اقدامات غیرفعال مانند مکان‌یابی مناسب سامانه‌های ارتباطی، واپایش انتشار[1]، استفاده از آنتن جهتی، مدیریت بسامد و فریب (Richard A. Poisel, 2004: 2).

۳-۱ اقدامات فعال محافظت الکترونیکی:

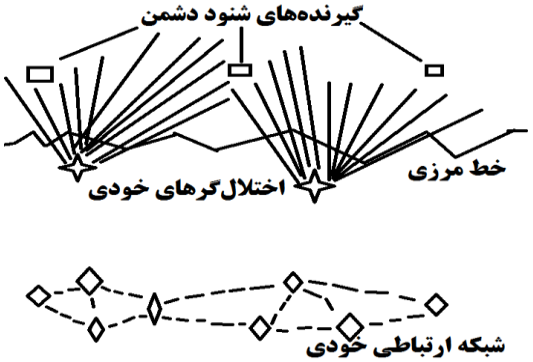
رمزنگاری: می‌توان پیامی را که در معرض ره‌گیری و شنود قرار دارد به‌گونه‌ای تغییر داد که در صورت کشف و ره‌گیری، داده‌های قابل‌استفاده‌ای برای دشمن نداشته باشد. این کار با رمزنگاری شدنی است(فیلیپونری، ۱۳۸۹: ۵۹۳). رمزنگاری علم نگهداری پیام‌ها و اطلاعات به‌صورت امن است. عملیات رمزنگاری زمانی مؤثر است که از تجهیزات و الگوریتم‌های رمز بومی استفاده شود.

فناوری‌های با احتمال کشف و آشکارسازی پایین[2]: سیگنال‌های ارتباطی با احتمال رهگیری پایین دارای مدولاسیون‌های خاصی هستند که به آن‌ها امکان می‌دهد طیف سیگنال خود را در بازهٔ زیادی از پهنای باند گسترش داده و به‌اصطلاح طیف گسترده ایجاد کنند. به همین دلیل سیگنال‌های

1. Emission Control (EMCON)
2. Low Probability Of Interception (LPI)

ارتباطی با احتمال ره‌گیری پایین را سیگنال‌های طیف گسترده نیز می‌نامند. این نوع سیگنال‌ها برای ارسال‌ها و ارتباط‌های ویژه، پنهان نمودن سیگنال‌های ارتباطی و حذف سیگنال‌های تداخلی ناخواسته استفاده می‌شوند. روش‌های با احتمال رهگیری پایین، امنیت ارتباطات را تأمین می‌کنند و باعث دشوارسازیِ کشف حضور سیگنال یا ره‌گیری و اختلال آن برای دشمن می‌شوند. البته این موضوع متفاوت از امنیت پیام است. امنیت پیام با اقدامات مربوط به رمزنگاری پیام‌ها انجام می‌شود (دیوید آدامی، ۱۳۹۲: ۷۷). برخی روش‌های با احتمال ره‌گیری پایین عبارت‌اند از: پرش بسامد[1]، دنباله مستقیم[2]، پرش زمانی و روش ترکیبی (Richard Poisel, 2011: 8-10).

اختلال پوششی: در اختلال پوششی سامانه اخلال‌گر بین شبکه ارتباطی خودی و ایستگاه جنگ الکترونیک دشمن قرار می‌گیرد. عملیات اختلال پوششی با اختلال عمدی بسامدهای نیروهای خودی با استفاده از آنتن‌های جهتی است که پرتو آن‌ها به‌سمت دشمن قرار دارد (Richard A. Poisel, 2002: 5). در شکل شماره ۶ هندسه اختلال پوششی نشان داده شده است.



شکل شماره ۶: هندسه اختلال پوششی.

چگونگی انجام اختلال به این صورت است که فهرست بسامدهای نیروهای خودی که لازم است از شنود آن‌ها به وسیله دشمن جلوگیری به‌عمل آید، به گروه مجری اختلال که مجهز به اختلال‌گرهای مناسب است واگذار می‌شود. با هماهنگی و زمان‌بندی مناسب، گروه اختلال با توانی مناسب شروع به ارسال سیگنال‌های اختلال در بسامد کاری نیروهای خودی به سمت گیرنده‌های شنود دشمن می‌کند. ازآنجایی‌که گیرنده‌ها همیشه سیگنال‌های قوی‌تر را دریافت می‌کنند، گیرنده‌های شنود دشمن به جای دریافت بسامد و سیگنال‌های شبکه ارتباطی نیروهای خودی، سیگنال‌های اختلال‌گرها را دریافت می‌کنند. به‌این‌ترتیب ارتباط‌های شبکه

1. Frequency Hopping (FH)
2. Direct Sequence (DS)

ارتباطی نیروهای خودی از شنود تا حد زیادی ایمن می‌ماند. اختلال پوششی اقدامی موقت و در عملیات ویژه مانند بازدیدهای مقامات از مناطق مرزی، رزمایش‌ها، عملیات ویژه، آزمایش عملیاتی سامانه‌های مهم و ... طراحی و اجرا می‌شود.

کدینگ منبع و کانال بومی: کدینگ‌های منبع و کانال، موفقیت عملیات شنود و اختلال دشمن را با مشکلاتی روبرو می‌کند. اگر به‌جای کدهای منبع و کانال استاندارد از کدهای بومی استفاده شود، عملیات کدگشایی آن برای سامانه رهگیر و شنود دشمن سخت‌تر خواهد بود.

۳-۲ اقدامات غیرفعال محافظت الکترونیکی:

مدیریت بسامد: به‌منظور استفاده مؤثر از طیف بسامدهای رادیویی و برخورداری از کمینه میزان تداخل، مدیریت طیف بایستی به‌صورت خودکار انجام شود. در صحنه نبرد نظامی که عملیات اختلال رادیویی، عملکرد و کارایی سامانه‌های ارتباطی را هدف قرار می‌دهد، انجام خودکار مدیریت طیف ضروری است. یکی از فناوری‌های نوین مدیریت طیف و بسامد فناوری رادیوشناختی است.

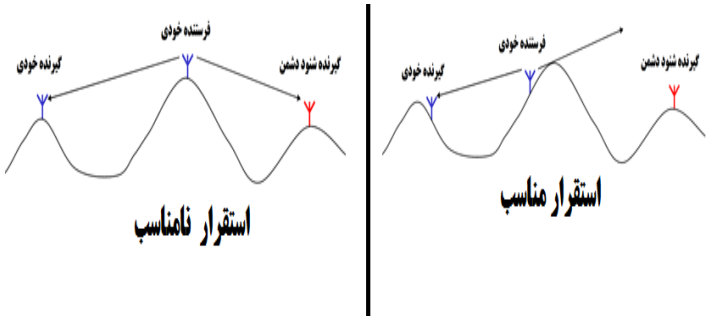
رادیو شناختی[1]: سازمان‌های واگذارکنندهٔ بسامد، طیف بسامدی را به کاربران مختلف واگذار می‌کنند؛ به این کاربران، کاربران اولیه[2] می‌گویند. شبکه‌های رادیوشناختی[3] به‌عنوان کاربران ثانویه[4] طیف عمل می‌کنند به شرطی که در آن زمان و مکان در ارتباط کاربران اولیه تداخلی ایجاد نشود. بدین منظور شبکه‌های رادیوشناختی بایستی به‌صورت متناوب طیف بسامدی را برای آشکارسازی فعالیت کاربران اولیه، پایش کند و به‌محض کشف فعالیت، باید کانال را برای ارتباط کاربران اولیه خالی کنند (زارع آغداش و همکاران، ۱۳۹۲: ۵).

مدیریت توان: یکی از روش‌های جلوگیری از انتشار سیگنال‌های رادیویی به‌سمت دشمن، استفاده از توان بهینه فرستنده ارتباطی است. توان و برد مؤثر سامانه ارتباطی با توان ارسالی متناسب است؛ بنابراین با کاهش توان فرستنده، برد انتشاری آن کاهش‌یافته و درنتیجه احتمال دریافت سیگنال از سوی دشمن نیز کاهش می‌یابد.

برپایی مناسب: برپایی سامانه‌های ارتباطی براساس انتشار امواج رادیویی بین ایستگاه‌های ارتباطی موردنظر طراحی و اجرا می‌شود. این طراحی باید به‌گونه‌ای باشد که دست‌یابی اقدامات پشتیبانی و تهاجم الکترونیکی دشمن به طیف امواج رادیویی خودی، کمینه شود. در این زمینه استفاده از عوارض زمین (با توجه به بازهٔ بسامدی مورد استفاده) اهمیت بسیار زیادی دارد. یکی

1. Cognitive Radio
2. Primary User
3. Cognitive Radio Networks (CRN)
4. Secondary User

از این روش‌ها پایین آوردن فرستنده‌های رادیویی ارتباطی از قله تپه‌ها است (مایکل رایان و همکاران، ۱۳۸۵: ۷۲). روش درست برپایی سامانهٔ ارتباطی در شکل شماره ۷ نشان داده شده است. امروزه برای برپایی مناسب سامانه‌های ارتباطی، از نرم‌افزارهای ویژه طراحی شبکه‌های ارتباطی و مکان‌یابی استفاده می‌شود.



شکل شمارهٔ ۷: برپایی مناسب سامانه‌های ارتباطی (مایکل رایان و همکاران، ۱۳۸۵: ۷۲).

آنتن‌های جهتی: آنتن وسیله‌ای است که انرژی الکتریکی را به انرژی رادیویی و برعکس تبدیل می‌کند. این وسیله امواج رادیویی را منتشر یا دریافت می‌کند. آنتن بین فضای آزاد و خط انتقال قرار می‌گیرد (Constantine A. Balanis, 2005: 2). آنتن‌ها با توجه به الگوی تشعشعی به دو دسته آنتن همه‌جهته (آنتن‌هایی که برای کار در همهٔ جهت‌ها طراحی شده‌اند) و آنتن جهتی (آنتن‌هایی که برای کار در جهتی خاص هستند) تقسیم می‌شوند (دیوید آدامی، ۱۳۸۵: ۳۸). در صورت استفاده از آنتن جهتی، تشعشع به سمت مطلوب است و سیگنال‌های کمتری به سامانه شنود دشمن می‌رسد. بهره‌گیری از آنتن جهتی یکی از اقدامات محافظت الکترونیکی به‌شمار می‌آیند.

آنتن هوشمند: استفاده از آنتن‌های هوشمند نیز یکی از روش‌های افزایش امنیت سیگنال در برابر شنود و تداخل است. با استفاده از روش‌های شکل‌دهی بیم، بیم آنتن تنها در راستای گیرنده ارسال می‌شود و از شنود دشمن ایمن می‌ماند. علاوه‌براین، استفاده از آنتن‌های هوشمند برتری‌های دیگری چون کاهش اثرات چندمسیری کانال، محوشدگی و همچنین کاهش اثرات تداخل ناخواسته و کاهش احتمال خطا را درپی دارد (نقوی، ۱۳۹۱: ۱۶).

فریب الکترومغناطیسی: فریب الکترومغناطیسی عبارت است از انتشار یا انتشار دوباره، دست‌کاری، کاهش، جذب، جلوگیری، تقویت یا بازتاب انرژی الکترومغناطیسی برای انتقال اطلاعات گمراه‌کننده به دشمن یا سلاح‌های الکترومغناطیس دشمن که باعث کاهش کارایی یا خنثی کردن توانمندی رزمی دشمن می‌شود (گروه مترجمان پژوهشکده پدافند غیرعامل، ۱۳۸۹: ۲۳ – ۲۴).

فریب الکترونیکی به سه دسته فریب الکترونیکی جعلی، فریب الکترونیکی شبیه‌سازی‌شده و فریب الکترونیکی تقلیدی تقسیم می‌شود. فریب الکترونیکی جعلی به قصد آسیب زدن به تجهیزات پشتیبانی الکترونیکی و اطلاعات سیگنالی دشمن با استفاده از اقدام‌هایی مانند تغییر مشخصات فنی فرستنده‌ها، رعایت نکردن اصول واپایش‌شده امنیتی، ارسال بیش‌ازحد بسته‌های اطلاعاتی برای ساختن یک اثر گمراه‌کننده از مخابره‌های بعدی، جابه‌جا کردن تجهیزات مخابراتی، تغییر در جریان ارسال‌ودریافت بسته‌های اطلاعاتی و ... انجام می‌شود (عفیفی و همکاران، ۱۳۸۵: ۱۹۹). فریب الکترونیکی شبیه‌سازی از امواج الکترومغناطیسی دروغین برای ساختن نمای یک نیرو، سامانه و فعالیت در یک موقعیت مکانی اشتباه بهره می‌گیرد. در فریب الکترونیکی تقلیدی، کاربران جنگال تلاش می‌کنند تا با وارد شدن به شبکه‌های ارتباطی دشمن و تقلید نمودن از ایستگاه‌های آن‌ها، دشمن را گمراه کرده یا اطلاعاتی به‌دست آورند (عفیفی و همکاران، ۱۳۸۵: ۱۹۹).

روش، نوع پژوهش، جامعه آماری و تجزیه‌وتحلیل داده‌ها

روش انجام این مقاله توصیفی – تحلیلی است که پس از گردآوری اطلاعات از منابع کتابخانه ای و مصاحبه با نخبگان حوزه ارتباطات و جنگ الکترونیک برخی یگان‌های نیروهای مسلح، با استفاده از ابزار پرسش‌نامه ساختهٔ پژوهشگر انجام شده است. اعتبار ابزار از دید متخصصان با استفاده از روش دلفی مورد تأیید قرارگرفته و پایایی آن نیز با استفاده از آزمون ضریب آلفای کرونباخ برای پرسشنامه ۹۱/۸۳ درصد تعیین شده است. جامعه آماری شامل تعداد چهارده نفر مدیران، چهل‌وشش نفر کارشناس و شصت نفر متخصصان فرماندهی جنگال ساحفاجا و معاونت فاوای آجا هستند که با استفاده از فرمول کوکران تعداد هفت نفر مدیر، نوزده نفر کارشناس و بیست‌وچهار نفر متخصص به‌عنوان جامعه نمونه آماری به‌دست آمده است.

روش تجزیه‌وتحلیل داده‌های پژوهش با بهره‌گیری از نرم‌افزارهای EXCEL و SPSS به دو شیوه توصیفی (جدول‌های توزیع فراوانی و ویژگی‌های آماری) و استنباطی (آزمون خی ۲ برای تأیید روابط بین متغیرها و آزمون t تک نمونه‌ای به‌منظور تأیید فرضیه‌ها) انجام و متغیرهای پژوهش نیز با استفاده از ابزار تحلیلی فریدمن اولویت‌بندی شده‌اند.

تحلیل داده‌های فرضیه اول: این فرضیه برای پاسخ به این سؤال تدوین شده که «هر یک از اقدامات فعال به چه میزان در برابر آسیب‌پذیری‌های کشف، شناسایی، شنود، سمت‌یابی، تعیین موقعیت و تحلیل ارسال‌ودریافت ارتباطات رادیویی مؤثر می‌دانید؟» تعداد نه پرسش در ارتباط با این فرضیه تنظیم و داده‌های آن‌ها از جامعه آماری جمع‌آوری شده است که ویژگی‌های آن‌ها در جدول شماره ۱ ثبت شده است.

جدول شمارهٔ ۱: ویژگی‌های داده‌های فرضیه اول

ویژگی	سؤال ۱	سؤال ۲	سؤال ۳	سؤال ۴	سؤال ۵	سؤال ۶	سؤال ۷	سؤال ۸	سؤال ۹
تعداد معتبر	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰
تعداد نامعتبر	۰	۰	۰	۰	۰	۰	۰	۰	۰
میانگین	۴.۶۴	۳.۹۲	۴.۳۶	۴.۳۲	۳.۹۸	۳.۸۸	۴.۰۴	۴.۲۶	۳.۹۸
میانه	۵	۴	۴	۴	۴	۴	۴	۴	۴
مد	۵	۴	۴	۴	۴	۴	۴	۴	۴
انحراف معیار	۰.۵۲۵	۰.۸۹۹	۰.۵۶۳	۰.۵۸۷	۰.۶۵۴	۰.۷۱۶	۰.۵۷۰	۰.۶۹۴	۰.۴۷۲
واریانس	۰.۲۷۶	۰.۸۰۹	۰.۳۱۷	۰.۳۴۵	۰.۴۲۳	۰.۵۱۶	۰.۳۲۵	۰.۴۸۲	۰.۵۵۰
کمینه	۳	۱	۳	۳	۳	۲	۳	۳	۳
بیشینه	۵	۵	۵	۵	۵	۵	۵	۵	۵

تحلیل توصیفی داده‌های فرضیه اول: نتایج آمار توصیفی داده‌های مربوط به فرضیه اول در جدول شماره ۲ ثبت شده است.

جدول شمارهٔ ۲: نتایج آمار توصیفی فرضیه اول

فرضیه اول	تعداد مشاهدات	میانگین	انحراف معیار
حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات فعال انجام می‌شود.	۵۰	۴.۱۵۳۲	۰.۴۰۶۶۳

متوسط پاسخ پاسخ‌دهندگان برابر ۴.۱۵۳۲ با انحراف معیار ۰.۴۰۶۶۳ است. این مقدار میانگین بیان‌کننده این نکته است که پاسخگویان بر این باورند که حفاظت ارتباطات رادیویی با به‌کارگیری اقدامات فعال انجام می‌شود.

برای تحلیل استنباطی داده‌های فرضیه اول از آزمون تی تک نمونه و مقدار آزمون برابر ۳ (سطح پاسخ متوسط) درنظر گرفته شده است.

H_0= نقیض ادعا: حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات فعال انجام نمی‌شود ($X\leq3$). ؛ **H_1= ادعا:** حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات فعال انجام می‌شود ($X>3$).نتایج به‌دست آمده از آزمون تی تک نمونه‌ای در جدول زیر ثبت شده است.

جدول ۳: نتایج آزمون تی تک نمونه‌ای فرضیه اول

فرضیه اول	مقدار آزمون >۳			
	t	درجه آزادی	سطح معناداری	تفاضل میانگین
حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات فعال انجام می‌شود.	۲۰.۰۵۴	۴۹	۰.۰۰۰	۱.۱۵۳۲

در این آزمون میزان آماره t برابر ۲۰.۰۵۴ با درجه آزادی ۴۹ و سطح معناداری ۰.۰۰۰ است. چون میزان سطح معناداری از میزان خطای نوع اول α در سطح ۰.۰۵ کمتر است بنابراین فرضیه اول با ۹۵ درصد اطمینان تأیید و به‌عبارت‌دیگر حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات فعال انجام می‌شود.

تحلیل داده‌های فرضیه دوم: این فرضیه برای پاسخ به این سؤال که «هر یک از اقدامات غیرفعال به چه میزان در برابر آسیب‌پذیری‌های کشف، شناسایی، شنود، سمت‌یابی، تعیین موقعیت و تحلیل ارسال‌ودریافت ارتباطات رادیویی مؤثر می‌دانید؟» تدوین شده است. تعداد هفت پرسش در ارتباط با این فرضیه تنظیم و داده‌های آن‌ها از جامعه آماری جمع‌آوری که ویژگی‌های آن‌ها در جدول شماره ۴ ثبت شده است.

جدول شماره ٤: ویژگی‌های داده‌های فرضیه دوم

ویژگی	سؤال ۱۰	سؤال ۱۱	سؤال ۱۲	سؤال ۱۳	سؤال ۱۴	سؤال ۱۵	سؤال ۱۶
تعداد معتبر	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰
تعداد نامعتبر	۰	۰	۰	۰	۰	۰	۰
میانگین	۴.۱۲	۴.۱۰	۴.۰۶	۴.۱۰	۴.۲۶	۴.۲۴	۴.۱۰
میانه	۴	۴	۴	۴	۴	۴	۴
مد	۴	۴	۴	۴	۴	۴	۴
انحراف معیار	۰.۷۱۸	۰.۶۱۴	۰.۶۱۲	۰.۶۷۸	۰.۶۶۴	۰.۶۲۵	۰.۶۷۷
واریانس	۰.۵۱۶	۰.۳۷۷	۰.۳۸۴	۰.۴۵۹	۰.۴۴۱	۰.۳۹۰	۰.۴۵۲
کمینه	۲	۳	۳	۳	۳	۲	۳
بیشینه	۵	۵	۵	۵	۵	۵	۵

تحلیل توصیفی داده‌های فرضیه دوم: نتایج آمار توصیفی داده‌های مربوط به فرضیه دوم در جدول شماره ۵ ثبت شده است.

جدول شماره ٥: نتایج آمار توصیفی فرضیه دوم

فرضیه دوم	تعداد مشاهدات	میانگین	انحراف معیار
حفاظت ارتباطات رادیویی در مقابل اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات غیرفعال انجام می‌شود.	۵۰	۴.۱۴۰۰	۰.۴۰۱۱۱

متوسط پاسخ‌های ارائه‌شده از سوی پاسخ‌دهندگان برابر ۴.۱۴۰۰ با انحراف معیار ۰.۴۰۱۱۱ است. میانگین بیان‌کننده این نکته است که پاسخگویان معتقدند که حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات غیرفعال انجام می‌شود.

تحلیل استنباطی فرضیه دوم: برای انجام و آزمون فرضیه از آزمون تی تک نمونه استفاده شده است. در این آزمون مقدار آزمون را برابر ۳ (سطح پاسخ متوسط) درنظر گرفته شده است.

H_0= نقیض ادعا: حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات غیرفعال انجام نمی‌شود ($X \leq 3$).

H_1= ادعا: حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات غیرفعال انجام می‌شود ($X > 3$). نتایج به‌دست آمده از آزمون تی تک نمونه‌ای در جدول شماره ۶ ثبت شده است.

جدول شماره ٦: نتایج آزمون تی تک نمونه‌ای فرضیه دوم

فرضیه دوم	مقدار آزمون >۳			
	T	درجه آزادی	سطح معناداری	تفاضل میانگین
حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی حریفان با به‌کارگیری اقدامات غیرفعال انجام می‌شود.	۲۰.۰۹۷	۴۹	۰.۰۰۰	۱.۱۴۰۰

در این آزمون میزان آماره t برابر ۲۰.۰۹۷ با درجه آزادی ۴۹ و سطح معناداری ۰.۰۰۰ است. چون میزان سطح معناداری از میزان خطای نوع اول α در سطح ۰.۰۵ کمتر است بنابراین فرضیه دوم با ۹۵ درصد اطمینان تأیید و به‌عبارت‌دیگر: حفاظت ارتباطات رادیویی برای مقابله با اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات غیرفعال انجام می‌شود.

اولویت‌بندی داده‌های فرضیه اول: حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات فعال انجام می‌شود. میزان تأثیرگذاری و امتیاز تعداد نه متغیر درباره فرضیه اول با بهره‌گیری از روش فریدمن تعیین و نتایج به‌دست آمده در جدول شماره ۷ ثبت شده است.

جدول شمارهٔ ۷: تحلیل فریدمن داده‌های فرضیه اول

اولویت	شرح سؤال	امتیاز
۱	رمزنگاری با بهره‌گیری از قراردادهای بومی	۶.۸۰
۲	استفاده از فناوری با احتمال ره‌گیری پایین (پرش فرکانسی، دنباله مستقیم و ...)	۵.۷۱
۳	استفاده از کدینگ و قراردادهای ارتباطی بومی	۵.۶۳
۴	استفاده از آنتن‌های هوشمند	۵.۴۰
۵	انتخاب خودکار بسامد و چابکی بسامد	۴.۵۰
۶	فریب رادیویی (وانمودسازی، تغییر ارسال‌ودریافت بسته‌ها و ...)	۴.۳۲
۷	استفاده از رله‌های هوشمند	۴.۳۲
۸	استفاده از جدول‌های کشف و رمز و کدهای اختصاری	۴.۲۳
۹	اختلال پوششی	۴.۰۹

اولویت‌بندی داده‌های فرضیه دوم: حفاظت ارتباطات رادیویی در برابر اقدامات پشتیبانی الکترونیکی با به‌کارگیری اقدامات غیرفعال انجام می‌شود. میزان تأثیرگذاری و امتیاز تعداد هفت متغیر درباره فرضیه دوم با بهره‌گیری از روش فریدمن تعیین و نتایج به‌دست آمده در جدول شماره ۸ ثبت شده است.

جدول شمارهٔ ۸: تحلیل فریدمن داده‌های فرضیه دوم

اولویت	شرح سؤال	امتیاز
۱	طراحی هوشمند شبکه‌های ارتباطی (بهره‌گیری از نرم‌افزارهای ویژه)	۴.۳۱
۲	استفاده از ابزارهای جایگزین مانند ارتباطات سیمی و پیک	۴.۲۸
۳	مدیریت توان	۴.۰۱
۴	برپایی سامانه ارتباطی در محل مناسب با استفاده بهینه از جغرافیای منطقه	۳.۹۵
۵	استفاده از آنتن‌های جهتی	۳.۸۴
۶	مدیریت طیف و بسامد	۳.۸۲
۷	تدوین و به‌کارگیری صحیح دستور کار مخابراتی	۳.۷۹

نتیجه‌گیری و پیشنهادها

اقدامات حافظت الکترونیکی سامانه‌ها و تجهیزات ارتباطی فرایندی همیشگی است که بایستی در مراحل طراحی، تولید سامانه (حوزه صنعت)، نگهداری و بهره‌برداری عملیاتی (حوزه نیروهای مسلح) و حتی پس از محافظت از اطلاعات سامانه‌ها، پایش اقدامات محافظتی انجام‌شده و ... درنظر گرفته شود. این اقدامات در دو دسته فعال و غیرفعال تقسیم‌بندی شده که با تقویت مشخصات امنیتی سامانه‌های ارتباطی، آنها را در برابر تهدیدهای حوزهٔ جنگ الکترونیک ایمن می‌کند. بر این اساس اقدامات فعال و غیرفعال زیر بیشترین نقش را در حافظت سامانه‌های ارتباط رادیویی در برابر اقدامات پشتیبانی الکترونیکی حریفان دارند:

الف) اقدامات فعال:

- رمزنگاری با الگوریتم‌های بومی سامانه‌ها و شبکه‌های ارتباطی را در برابر شنود محافظت می‌کند.
- استفاده از فناوری با احتمال ره‌گیری پایین مانند روش‌های طیف گسترده پرش بسامدی، دنباله مستقیم و روش‌های ترکیبی عملیات کشف، شناسایی و آشکارسازی سیگنال سامانه‌های ارتباطی را برای سامانه‌های جنگ الکترونیک دشمن سخت نماید.
- استفاده از کدینگ و قراردادهای ارتباطی بومی، دست‌یابی به محتوای ارتباطات را برای دشمن سخت‌تر می‌کند.

- اختلال پوششی موقت و راهکنشی است که در عملیات ویژه مانند رزمایش‌ها، آزمایش سامانه‌های جدید، بازدیدهای مقامات از مناطق مرزی و... طراحی و اجرا می‌شود.

ب) اقدامات غیرفعال:

- طراحی هوشمند شبکه‌های ارتباطی با استفاده از نرم‌افزارهای تخصصی به طراحان شبکه‌های ارتباطی در پیاده‌سازی عملی شبکه‌ها، شبیه‌سازی اقدامات جنگ الکترونیک حریفان و ارزیابی راه‌کارهای محافظت ارتباطات کمک می‌کند.
- استفاده از ابزارهای جایگزین چون ارتباطات سیمی پایداری جریان اطلاعات را تضمین می‌کند.
- مدیریت توان و برپایی سامانه ارتباطی در محل مناسب با استفاده بهینه از جغرافیای منطقه با واپایش انتشار سیگنال، مانع از رسیدن سیگنال سامانه‌های ارتباطی به سامانه‌های جنگ الکترونیک دشمن می‌شود.

در پایان پیشنهادهایی در دو حوزهٔ صنعت و نیروهای مسلح به‌شرح زیر ارائه می‌گردد:

الف-حوزهٔ صنعت (سازمان‌های جهاد خودکفایی نیروهای مسلح، وزارت دفاع و پشتیبانی نیروهای مسلح و شرکت‌های فناوری داخلی):

- طراحی و تولید سامانه‌های ارتباطات رادیویی با فناوری‌های با احتمال ره‌گیری پایین مانند پرش بسامدی، پرش زمانی، دنباله مستقیم، ترکیبی، ارسال انفجاری
- تولید سامانه‌های رمزکننده با الگوریتم‌های بومی مورد تأیید ستاد کل نیروهای مسلح
- طراحی و پیاده‌سازی فناوری‌های نوین محافظت ارتباطی مانند شبکه‌های رادیو شناختی[1] و آنتن هوشمند.

ب) حوزهٔ نیروهای مسلح:

- ایجاد مرکزهای پایش فناوری‌های نوین ارتباطی، شناسایی تهدیدها و روش‌های مقابله‌ای با تهدیدها
- طراحی هوشمند شبکه‌های ارتباط رادیویی و بهره‌گیری از نرم‌افزارهای شبیه‌ساز ارتباط رادیویی برای شبیه‌سازی اقدامات جنگ الکترونیک و ارزیابی راه‌کارهای خودی.
- به‌روز نمودن مستندات و موضوع‌های آموزش امنیت ارتباطات متناسب با تهدیدهای نوین و به‌کارگیری و ارزیابی آموزش‌های ارائه‌شده در رزمایش‌های عمومی و تخصصی جنگ الکترونیک.

1. Cognitive Radio Networks (CRN)

منابع

۱.ابراهیمی، اصغر و همکاران. (۱۳۹۰)، ***جو زمین و اثرات آن بر امواج الکترومغناطیس***، تهران: انتشارات ناقوس، پژوهشکده گروه صنایع فضایی صاایران.

۲.آدامی، دیوید. (۱۳۸۵)، ***جنگ الکترونیک (EW 101)***، نایبی، محمدمهدی، تهران: دانشگاه شریف.

۳.آدامی، دیوید. (۱۳۹۲)، ***جنگ الکترونیک ارتباطی در فضای تاکتیکی میدان نبرد***، موسوی، سید نواب، تهران: انتشارات دانشکده علوم و فنون فارابی.

۴.اسکندری، حمید. (۱۳۹۰)، ***دانستنی‌های پدافند غیرعامل***، تهران: انتشارات بوستان حمید.

۵.پالی، جوزف‌س. (۱۳۷۴)، ***مخابرات فیبرنوری***، ترجمه: مولوی، محمد، محدث، مجتبی، مشهد: دانشگاه امام رضا (ع).

۶.جلالی فراهانی، غلامرضا. (۱۳۹۰)، ***پدافند غیرعامل و تهدیدات نوین***، تهران، بوستان حمید.

۷.چاندرا، پراپهول. (۱۳۸۸)، ***امنیت در شبکه‌های رایانه‌ای و مخابراتی بی‌سیم***، مترجمین: ریاضی، عباس و همکاران، تهران: انستیتو ایز ایران.

۸.دهقانی، مصطفی، موسوی، سید نواب. (۱۳۹۰)، ***مقاله نقش جنگ الکترونیک در عملیات ناتو، سقوط و مرگ قذافی***، پنجمین همایش ملی جنگ الکترونیک ایران، تهران: دانشگاه جامع امام حسین (ع).

۹.زارع آغداش، صابر، دهقانی، مصطفی، جهانشاهلو، حمیدرضا. (۱۳۹۲)، ***بهبود سنجش طیف مشارکتی در ارتباطات رادیو شناختی با انتخاب پارامترهای بهینه***، ششمین همایش ملی جنگ الکترونیک ایران، تهران: دانشگاه جامع امام حسین (ع).

۱۰.سنگرگیر، مراد، جواهری، علیرضا. (۱۳۹۱)، ***فرهنگ تشریحی جنگ الکترونیک***، تهران: مؤسسه آموزشی و پژوهشی صنایع دفاعی.

۱۱.فراتر، مایکل، رایان، مایکل. (۱۳۸۵)، ***جنگ الکترونیک برای صحنه نبرد دیجیتال***، مترجمین عفیفی، احمد و همکاران، تهران: مؤسسه آموزشی و پژوهشی صنایع دفاعی.

۱۲.فیلیپو نری. (۱۳۸۹)، ***مقدمه‌ای بر سامانه‌های دفاع الکترونیکی***، مترجمین: نایبی، محمدمهدی و نیک‌اندیش، غلامرضا، تهران: مؤسسه آموزشی و پژوهشی صنایع دفاعی.

۱۳.قاسمی، عبدالله. (۱۳۸۵)، ***مهندسی انتشار امواج رادیویی***، تهران: دانشگاه صنعتی امیرکبیر.

۱۴.گروه مترجمان دانشکده و پژوهشکده پدافند غیرعامل. (۱۳۸۹)، ***فریب نظامی***، تهران: دانشگاه جامع امام حسین (ع).

۱۵.نقوی، محمدتقی. (۱۳۹۱)، بررسی افق و چشم‌انداز شبکه‌های مخابراتی، ***فصلنامه تخصصی رعد*** شماره ۴ زمستان ۱۳۹۱، تهران: دانشگاه جامع امام حسین (ع).

۱۶.نیروی هوایی آمریکا. (۱۳۹۰)، سند دکترین نیروی هوایی آمریکا، ***دکترین جنگ الکترونیک مشترک***، موسوی، سید نواب، تهران: انتشارات دانشکده علوم و فنون فارابی
۱۷.واحدی، مرتضی.(۱۳۹۰)، **کلیات جنگ الکترونیک**، تهران: انتشارت دانشکده علوم و فنون فارابی
18. Adamy, David, (2011), **EW Pocket guide**, scitech, USA.
19. Adrian Graham, (2011), **Communications, RADAR and Electronic Warfare**, A John Wiley and Sons, Ltd, UK.
20. BERNARD SKLAR, (2000), **Digital Communications Fundamentals and Applications Second Edition**, Tarzana, California and University of California, Los Angeles, USA.
21. Constantine A. Balanis, (2005), **ANTENNA THEORY ANALYSIS AND DESIGN (THIRD EDITION)**, John Wiley & Sons, Inc. Hoboken, New Jersey.
22. MARTIN H. BARRINGER, (2013), **Radio Wave Propagation**.
23. Michael Frater and Michael Ryan,(2001), **Communications Electronic Warfare and the Digitized Battlefield**, Land Warfare Studies Centre, Australia.
24. Richard Poisel, (2002), **Introduction to Communication Electronic Warfare Systems**, ARTECH HOUSE, UK.
25. Richard Poisel, (2004), **Target acquisition in communication electronic warfare systems**, ARTECH HOUSE, UK.
26. Richard Poisel, (2011), **Modern Communications Jamming Principles and Techniques Second Edition**, ARTECH HOUSE, UK.
27. Roger J. Sutton,(2002), **Secure Communications: Applications and Management**, John Wiley & Sons, Ltd, England.
28. S. Deakin, Richard,(2010), **BATTLESPACE TECHNOLOGIES: Network-Enabled Information Dominance**, ARTECH HOUSE, USA.
29. Terry, I. (2003). "**US Naval Research Laboratory - Networked Specific Emitter Identification in Fleet Battle Experiment Juliet**"(http:/ / www.nrl. navy. mil/ content). NRL Review.. Retrieved 2007-10-26.