

راه کارهای عملیاتی (تاکتیکی) مقابله با جنگ در رادارهای هشدار اولیه با رویکردهای مدیریتی

محمدحسین برجسته باف^{۱*}

۱، * - دانشجوی کارشناسی ارشد مدیریت

چکیده

با توجه به تکنولوژی بالای دشمن در جنگ الکترونیک، این موضوع یکی از تهدیدات بالقوه علیه کشور است. سامانه‌های راداری و مخصوصاً رادارهای هشدار اولیه به دلیل اهمیت آن‌ها در مراحل اولیه جنگ جهت رصد اهداف دشمن، دائم در معرض خطر حملات الکترونیکی و جنگ الکترونیک بوده‌اند. سؤال اصلی در این مقاله این است که راهکارهای مقابله با جنگ الکترونیک در رادارهای هشدار اولیه چیست؟ در پاسخ به سؤال فوق، این مقاله با هدف تبیین روش‌هایی از مقابله اخلاص الکترونیک که کمتر راجع به آن شنیده‌اید و یا کمتر به آن توجه شده است، ارائه شده است. این مقاله از یک سو روش‌های اخلاص الکترونیک علیه رادارهای هشدار اولیه، آسیب‌پذیری‌ها، محدودیت‌ها و نقاط ضعف آن‌ها به صورت اجمال‌ی بیان می‌کند و از سویی دیگر راهکارهای مقابله موردبررسی قرار داده است. در آخر، بهترین راهکارهای مقابله‌ای با رویکرد عملیاتی (تاکتیکی) ارائه گردیدند. البته تلاش شده تا به موضوعات مدیریتی و تاکتیکی که بایستی در کنار موضوعات فنی، مکمل یکدیگر باشند، بیشتر توجه شود. این موضوع به این معنی است که راه کارهای مقابله با اخلاص الکترونیک همیشه راهکارهای فنی و پیچیده نیست، بلکه در کنار توجه به موضوعات فنی و علمی، با رفع برخی اشکالات ساده و توجه به مسائل جانبی جنگ الکترونیک، می‌توان در بخش مقابله به توفیقات زیادی دست یافت.

واژگان کلیدی: رادار هشدار اولیه، جنگ الکترونیک، فریب الکترونیک، روش‌های فنی مقابله با اخلاص الکترونیک، روش‌های عملیاتی مقابله با اخلاص الکترونیک

۱- مقدمه

از همان ابتدای ظهور مفاهیم الکترونیک و الکترومغناطیس، موضوعات جنگ الکترونیک به اشکال مختلف مطرح و به کارگیری شد. در سال‌های اخیر با توجه به گسترش سریع و روزافزون کاربرد تجهیزات الکترونیکی و نیز تجهیزاتی که با طیف امواج الکترومغناطیس سروکار دارند، به سرعت جنگ الکترونیک طیف وسیعی از کاربردها مخصوصاً در حوزه سایبر و الکترومغناطیس را دربر گرفته و در همین راستا اهمیت ویژه‌ای در محاسبات دفاعی و طرح‌ریزی‌های عملیاتی پیدا کرده است.

یکی از تجهیزات بسیار پراهمیت و پرکاربرد در حوزه دفاعی و به‌ویژه در بخش پدافند هوایی هر کشور، رادارهای هشدار اولیه می‌باشند که به دلیل اساس عملکرد آن‌ها که بر پایه ارسال و دریافت امواج الکترومغناطیس می‌باشد، در حوزه جنگ الکترونیک آسیب‌پذیری بالایی دارند، در نتیجه معمولاً در ساخت رادارها مورد این موضوع مورد توجه قرار گرفته و سعی بر کاهش اثرات جنگ الکترونیک بر روی این تجهیزات می‌گردد. در همین خصوص قابلیت‌ها و امکانات سخت‌افزاری و نرم‌افزاری به تناسب و تا حد امکان بر روی این تجهیزات پیش‌بینی شده، اما به دلیل عدم تکامل، به‌روز نبودن در برخی از رادارها، نداشتن تاکتیک به کارگیری و عدم توجه به مسائل جانبی به‌ویژه موضوعات عملیاتی در طرح‌های مقابله با جنگ الکترونیک، راه کارهای مقابله‌ای تا حدی کارایی خود را از دست داده‌اند. با توجه به اینکه از یک طرف یکی از توانمندی‌های عمده دشمن در نبردهای هوایی بهره‌گیری از روش‌های اخلال الکترونیک علیه تجهیزات طرف مقابل است و از طرف دیگر یکی از تجهیزات مهم خودی در خط مقدم دفاع، تجهیزات الکترونیکی و مخصوصاً رادارهای هشدار اولیه می‌باشند. لذا شناخت و تبیین روش‌های مختلف جنگ الکترونیک و توانمندی‌های فنی رادارها جهت مقابله با این تهدیدات، همچنین یافتن راهکارهای تاکتیکی در این خصوص از اهمیت ویژه‌ای برخوردار است.

۲- بیان مسئله

موضوع جنگ الکترونیک به عنوان یکی از موضوعات و مفاهیم مهم، گسترده و پیچیده در نبردهای اخیر همواره مورد توجه کارشناسان و خبرگان علوم نظامی قرار گرفته است. دلیل این اهمیت، تأثیر بسیار بالای توانمندی‌های جنگ الکترونیک در سرنوشت جنگ‌ها و تغییر معادلات و محاسبات طرف مقابل بوده است. از طرفی با توجه به گستردگی بسیار زیاد کاربردهای جنگ الکترونیک و توسعه روزافزون حوزه‌های مختلف آن در بخش تاکتیک و تکنیک، نمی‌توان در یک مطلب محدود به تمام ابعاد و ویژگی‌های جنگ الکترونیک پرداخت.

با عنایت به مطالب پیش‌گفته، واضح است که بایستی به ابعاد مختلف موضوع به صورت جداگانه و تخصصی پرداخت تا بتوان به نتیجه مطلوب دست پیدا کرد. در بین سامانه‌های راداری، سامانه‌های راداری هشدار اولیه به دلیل جایگاه مهمی که در اعلام هشدار شروع جنگ و رصد تحرکات دشمن دارند، از جایگاه ویژه‌ای برخوردارند و بایستی تأثیر جنگ الکترونیک بر این رادارها و راهکارهای مقابله با این

تأثیرات به صورت تخصصی و ویژه مورد بررسی قرار گرفته و تدوین گردد. لذا همواره این مسئله مطرح است که راهکارهای مقابله با جنگ الکترونیک در رادارهای هشدار اولیه کدام چیست؟

۳- مبانی نظری و ادبیات تحقیق

برای ایجاد اختلال الکترونیک در رادارها راه کارهای مختلفی چه در بخش فریب و چه در بخش اختلال وجود دارد، از قبیل، ^۱Spot Noise jamming، ^۲Barrage jamming، ^۳Swept spot jamming، ^۴Multiple spot jamming، فریب زاویه، فریب سرعت، جمینگ کناره (Skirt jamming)، اختلال پلاریزاسیون متقاطع (Cross polarization jamming)، دکوهای فریب. همچنین راه کارهای فنی بسیار زیادی مثل کنترل زمانی حساسیت گیرنده (STC)، ثابت زمانی سریع (FTC)، محو گلبرگ جانبی (SLB)، حذف گلبرگ جانبی (SLC)، پرش فرکانس، استفاده از فیلتر کالمن، استفاده از آنتن کمکی، تغییر PRF و بسیاری از تکنیک های فنی چه در بخش اختلال و چه در بخش مقابله وجود دارد که توضیح همه این ها در این مقاله امکان پذیر نیست. هدف ما نیز در این مقاله توضیح روش های متنوع جنگ الکترونیک و یا بیان راه کارهای پیچیده مقابله با آن نمی باشد زیرا برای شرح این موضوع باید به منابع متعددی که در این خصوص وجود دارد مراجعه نمود. البته باید تأکید کرد همه این موارد موضوعات بسیار مهمی هستند که حتماً باید به آن ها به صورت جدی توجه شود، اما در اینجا می خواهیم به جنبه های دیگری از اختلال الکترونیک بپردازیم که کمتر به آن ها توجه می شود و البته همین موضوعات تأثیر بسیار زیادی بر قابلیت های فنی مقابله با اختلال الکترونیک در رادارها می گذارد، تا جایی که ممکن است عدم توجه به آن ها، همه ی قابلیت های فنی رادار برای مقابله را تحت تأثیر قرار دهد. واضح است، همان گونه که روش های زیادی برای ایجاد اختلال الکترونیک در رادارها وجود دارد راه های مقابله ای زیادی در برابر آن ها وجود دارد، اما موضوع بسیار مهم، اتخاذ تاکتیک مقابله ای متناسب است. در نتیجه در اینجا طرفی موفق خواهد بود که بتواند در تاکتیک به کارگیری روش های جنگ الکترونیک، بهتر عمل نماید و بهترین روش را انتخاب کند. در این خصوص موضوعات مهمی وجود دارد که در ادامه به برخی از این موارد اشاره می کنیم و سپس پیشنهادهایی را نیز ارائه می کنیم.

۴- روش تحقیق

با توجه به موضوع مقاله که کاملاً علمی، فنی، تخصصی و از نوع کاربردی است، روش تحقیق کتابخانه ای در تهیه آن مورد استفاده قرار گرفته است. در این مقاله سعی شد جمع آوری اطلاعات با

^۱ جمینگ نقطه ای

^۲ جمینگ جاروبی

^۳ جمینگ جاروبی باریک

^۴ جمینگ چند نقطه ای

مطالعه دقیق بر روی منابع مرتبط داخلی و بین‌المللی، مقالات متعدد و سایت‌های داخلی و خارجی، با استفاده از روش فیش برداری انجام شود.

۵- یافته‌های تحقیق

- با توجه به گستردگی حوزه‌های الکترونیک و به‌کارگیری وسیع تجهیزات الکترونیکی و راداری در میان ارتش‌های دنیا، در حال حاضر جنگ الکترونیک جایگاه ویژه‌ای در میان نبردهای نظامی داشته و حتی می‌تواند به تنهایی بخش مستقلی از جنگ باشد. به عبارت دیگر نبردهای آتی حتماً در فضای جنگ الکترونیک خواهد بود. حال با توجه به نقش رادارها در جنگ‌های امروزی که در بستر آسمان انجام می‌شود، حفظ عملکرد این آن‌ها در شرایط مطلوب، اهمیت دوچندان پیدا کرده و بایستی حتماً مدنظر قرار گیرد.

- جنگ‌ها در آینده و نیز در حال حاضر، حتماً جنگ‌های ترکیبی (هیبریدی) هستند و علم و آگاهی به روش‌های جنگ الکترونیک و روش‌های مقابله با آن، نقش بسیار زیادی در تعیین سرنوشت جنگ‌ها دارد. تا جایی که ممکن است، طرفی که امکانات سخت‌افزاری زیادی دارد، به دلیل ضعف در احاطه به علوم جنگ الکترونیک و راه‌های مقابله‌ای، در جنگ با شکست مواجه شود و البته باید گفت که عکس این موضوع هم ممکن است اتفاق بیافتد.

- یکی از موضوعات مهم دیگر در جنگ الکترونیک، جنبه‌های تاکتیکی مقابله با اختلال الکترونیک می‌باشد. به این معنا که می‌توان با استفاده از راهکارهای تاکتیکی نسبتاً ساده، بسیاری از تکنیک‌های اختلال الکترونیک را به‌ویژه برای مقابله با اختلال در برابر رادارها استفاده کرد که در این خصوص توضیحات بیشتری خواهیم داد.

- تسلط به تکنیک‌ها و تاکتیک‌های جنگ الکترونیک و به‌کارگیری آن‌ها در تجهیزات، علاوه بر اینکه باعث افزایش کیفیت در توان تجهیزات خودی می‌گردد و می‌تواند دشمن را در اجرای عملیات اختلال ناکام نماید، می‌تواند با شناخت جنبه‌های مختلف دانشی و علمی در این حوزه منجر به تسلط به توانمندی‌های دشمن در زمینه جنگ الکترونیک گردد. لذا در نهایت می‌توان با علم و اشراف به این روش‌ها، به‌صورت دقیق اقدام نمود و ضربات سنگینی با تاکتیک‌های جنگ الکترونیک به دشمن وارد نمود.

- هر چه قدر که روش‌های اختلال الکترونیک متنوع و زیاد است، در عوض راه‌های مقابله نیز دارای تنوع بوده در صورت استفاده درست می‌توان به‌راحتی با بسیاری از اقدامات جنگ الکترونیک مقابله کرد؛ اما موضوع مهم در اینجا راه و روش به‌کارگیری تاکتیک‌های مقابله‌ای می‌باشد و این موضوع مهم هرگز بدون انجام آموزش‌های دقیق و کاربردی اتفاق نمی‌افتد. نکته جالب این است که اگر در به‌کارگیری تکنیک‌های مقابله هوشمندانه و بر اساس آموزش‌های دقیق عمل نشود، نه‌تنها مشکلی را حل نخواهد کرد، بلکه خود می‌تواند رادار را بیشتر در معرض خطر اختلال قرار دهد.

- حوزه جنگ الکترونیک موضوع جدیدی نیست اما روش‌های اخلاص و راه‌های مقابله دائماً به‌روز می‌گردد. همین موضوع مؤید نیاز به توجه جدی و مستمر به موضوع جنگ الکترونیک است. بسیاری روش‌های جنگ الکترونیک که درگذشته کاربرد داشته، هم‌اکنون و برخلاف پیشرفت‌های زیاد فناوری، همچنان کاربرد وسیعی دارند. به‌عنوان نمونه روش‌های اخلاص نویزی که جزء ساده‌ترین روش‌های اخلاص می‌باشد، همچنان کاربرد زیادی دارد و سامانه‌های راداری را می‌تواند با مشکل جدی مواجه نماید. پس در طراحی سامانه‌های راداری و طرح‌های دفاعی و حتی تهاجمی، باید به همه ابعاد جنگ الکترونیک توجه کرد.

- اخلاص الکترونیک هم می‌تواند به‌صورت نویزی انجام شود و هم می‌تواند به‌صورت فریب اتفاق بیافتد؛ اما نکته مهم این است که در حال حاضر، عموماً روش‌های فریب مورد توجه قرار گرفته و استفاده می‌شود، زیرا در بیشتر مواقع، طرف مقابل متوجه انجام عملیات اخلاص نمی‌شود. پس روش فریب هوشمندانه‌تر بوده و برای مقابله با آن باید هوشمندانه عمل کرد.

- با توجه به گسترش شبکه‌های ارتباطی در واحدهای مختلف نظامی و به‌ویژه شبکه‌های راداری، می‌توان نتیجه گرفت یکی از حوزه‌هایی که با موضوع اخلاص الکترونیک کاملاً مرتبط بوده و نمی‌توان آن‌ها را از هم جدا کرد، موضوع سایبر و فضای سایبر الکترومغناطیس است. موضوع استفاده از بستر سایبر الکترومغناطیس در اخلاص الکترونیک، بحث نسبتاً جدیدی است که در حال توسعه می‌باشد. اگرچه مقابله با این بستر نسبتاً پیچیده و با استفاده از روش‌های ترکیبی می‌باشد، اما نباید هرگز از این موضوع غافل شد.

۶- نتیجه‌گیری

۱- موضوع ارتقاء آموزش‌ها در حوزه جنگ الکترونیک، حتماً جزء پیشنهادهای اصلی می‌باشد. نگاه مختصر به آموزش در بخش جنگ الکترونیک، بعضاً سبب می‌شود تا کاربران نتوانند در مواجهه با اخلاص الکترونیک به‌خوبی عمل کنند. این بدان معناست که هر چه قدر در سامانه‌های راداری، قابلیت‌های مقابله‌ای پیش‌بینی شود، ولی کاربر آموزش کافی در استفاده از این قابلیت‌ها را ندیده باشد، نمی‌تواند از آن‌ها به‌خوبی استفاده کند. علاوه بر این عدم آموزش کافی در استفاده از قابلیت‌های مقابله‌ای رادار، حتی ممکن است وقتی رادار در شرایط اخلاص الکترونیک قرار می‌گیرد، نه‌تنها کاربر نمی‌تواند کمکی به بهبود شرایط کند، بلکه شرایط سخت‌تری را ایجاد نماید. لذا آموزش کامل و کاربردی در حوزه جنگ الکترونیک و تمرین مداوم در این خصوص حتماً بایستی توسط برنامه ریزان و مسئولین آموزشی مدنظر قرار گیرد.

۲- توجه به موضوع جنگ الکترونیک در همان ابتدای طراحی سامانه‌های راداری اهمیت بسیار زیادی دارد، چراکه بخش‌های مختلف یک سامانه راداری اعم از مکانیک، الکترونیک، پردازش و سایر اجزا نقش مهمی در روش‌های مقابله با اخلاص الکترونیک ایفا می‌کنند و بایستی باهم هماهنگی کامل داشته باشند. به این معنا که مثلاً اگر در بخش پردازش طراحی به‌خوبی انجام شود ولی در بخش مکانیک یا

آنتن اشکال وجود داشته باشد، سایر توانمندی‌های رادار تحت شعاع قرار گرفته و نمی‌تواند به‌خوبی عمل نماید. پس حضور یک کارشناس خبره جنگ الکترونیک در بخش‌ها و مراحل مختلف طراحی، موضوع بسیار مهمی است که باید مدنظر قرار گیرد. همچنین پیشنهاد می‌شود در پیوست فنی رادارها، پیوست جنگ الکترونیک به‌صورت کامل و جداگانه وجود داشته باشد.

۳- بهینه‌سازی رادارها نیز می‌تواند کمک بسیار زیادی به ارتقاء توانمندی‌ها در مقابله با جنگ الکترونیک ایجاد نماید. با توجه به اینکه تاریخ تولید برخی از رادارهایی که در حال حاضر در شبکه راداری به‌صورت عملیاتی در حال بهره‌برداری می‌باشند، مربوط به سال‌ها قبل می‌باشد و پیشرفت‌ها در بخش جنگ الکترونیک به‌سرعت اتفاق می‌افتد، در نتیجه، بهینه‌سازی این رادارها به‌ویژه در بخش‌های الکترونیکی و پردازشی می‌تواند بسیار مفید و راه‌گشا باشد.

۴- ممکن است در برخی از شرایط خاص، لازم نباشد در مقابل اختلال انجام‌شده بر روی رادار، واکنشی نشان دهیم، چراکه گاهی دشمن اقداماتی از نوع اختلال الکترونیک را به‌صورت هدفمند و هوشمندانه انجام می‌دهد تا واکنش طرف مقابل را رصد نماید. در نتیجه علاوه بر اینکه توانمندی خودی در این خصوص برای او آشکار خواهد شد، می‌تواند میزان تأثیرگذاری اختلال انجام‌شده بر روی رادار را مشاهده تا برای نبرد اصلی برنامه‌ریزی نماید. البته حتماً باید توجه داشت که انتخاب روش درست بایستی هوشمندانه و با در نظر گرفتن همه ملاحظات و امکانات خودی صورت پذیرد. به‌عنوان مثال اگر در شرایط جنگ منطقه‌ای خاص، توسط ۲ یا چند سامانه راداری هشدار اولیه پوشش داده می‌شود، یکی از رادارها مورد اختلال قرار گرفت، می‌توان بدون انجام هرگونه واکنشی، منطقه را توسط رادارهای دیگر رصد نمود، اما اگر فقط یک رادار منطقه را پوشش می‌دهد، بایستی حتماً به‌صورت مؤثر با آن مقابله نمود.

۵- نکته بسیار مهم دیگر که می‌توان در قسمت نتایج ذکر کرد، این است که استفاده ترکیبی از روش‌های مقابله با اختلال الکترونیک، احتمال موفقیت رادارهای خودی را در برابر تکنیک‌های اختلال تا حد زیادی افزایش می‌دهد. به این معنا که بسیاری از روش‌های مقابله‌ای مکمل یکدیگر هستند و بایستی به‌صورت هم‌زمان بکار گرفته شوند.

۶- با در نظر گرفتن تنوع و پیچیدگی انواع روش‌های اختلال الکترونیک و نیز روش‌های مقابله‌ای، به این نتیجه می‌رسیم که هر چقدر بتوانیم مقابله با اختلال الکترونیک را هوشمند کنیم، تأثیر اقدامات مقابله‌ای دوچندان می‌شود، چرا که شاید همیشه برای کاربر در نظر گرفتن همه ملاحظات و تصمیم‌گیری در زمانی کوتاه ممکن نباشد. بهترین راه برای هوشمند سازی در مقابله با اختلال الکترونیک، ایجاد قابلیت‌های خودکار در تشخیص و مقابله با اختلال الکترونیک می‌باشد و شاید این موضوع، مهم‌ترین پیشنهاد در این مقاله باشد. یعنی باید به سمتی حرکت کرد که وجود اختلال الکترونیک در رادار، تا حد ممکن به‌صورت خودکار تشخیص داده شده و به‌صورت خودکار و با کمترین دخالت کاربر با آن مقابله شود. البته حتماً باید در عین عملکرد خودکار، امکان تصمیم و دخالت کاربر وجود داشته باشد، تا در مواقعی که بنا به شرایط خاص، نیاز به اخذ تصمیم مجزا توسط کاربر است، این

امکان فراهم باشد، و در این شرایط، سیستم تشخیص خودکار فقط بایستی مانند یک مشاور، بهترین راه کارها را پیشنهاد دهد ولی کاربر تصمیم گیرنده نهایی باشد.

۷- شبکه محوری، مؤلفه دیگری از نبردهای هوشمند می باشد که هم برای طرف خودی از اهمیت بالایی برخوردار است و هم برای دشمن. اهمیت وجود شبکه کارآمد در جنگ الکترونیک دوچندان می شود، زیرا اقدامات مقابله با اختلال الکترونیک در صورت عدم اجرای مدیریت شده نه تنها مشکلی را حل نمی کند، بلکه ممکن است عملکرد رادارهای خودی را تضعیف نماید. پس نتیجه می گیریم که بایستی نگاه مدیران و کارشناسان طراح جنگ به موضوع شبکه محوری و مدیریت هوشمند صحنه نبرد کاملاً معطوف باشد.

۸- پیشنهاد آخر استفاده از جنگ الکترونیک در مقابل جنگ الکترونیک می باشد. یعنی در مواقعی خاص و به ویژه زمانی که تجهیزات و پرنده های جمع آوری دشمن در حال فعالیت می باشند، بدون اینکه نیاز به استفاده از روش های پیچیده مقابله با جنگ الکترونیک در رادارها باشد، می توان با استقرار دکوهای فریب (سامانه ای فریب با سیگنال هایی مشابه سامانه اصلی)، دشمن را در جمع آوری اطلاعات ناکام گذاشت تا در ادامه بتوان بخش زیادی از توان دشمن را صرف مقابله با این تجهیزات کرد. البته باید توجه داشت، همین روش ساده اگر به صورت هوشمندانه و مشابه حالت های واقعی اجرا شود، تشخیص فریب بودن آن را تقریباً غیر ممکن می سازد.

۷- منابع و مراجع

- [۱] تیموری، محمدرضا (۱۳۹۱)، بررسی انواع جمینگ در سامانه های راداری و راه های مقابله با آن، تهران، دانشگاه هوافضای عاشورا
- [۲] اکبرزاده، هومن، سرافراز، حمیدرضا، رسولی، حسن و طلعتی، سعید، (۱۳۹۶)، بررسی اختلال راداری و روش های نوین جمینگ سیگنال، تهران، دانشگاه هوافضای عاشورا
- [۳] حسینی نیا، امیر و معصومی، امیر (۱۳۹۰)، جمینگ در رادار، زنجان، دانشگاه زنجان
- [۴] سبحانی، جبار (۱۳۸۵)، اصول رادار، تهران، دانشگاه هوافضای عاشورا
- [۵] تابان، محمدرضا و شیخ مظفری، آرش (۱۳۹۳)، آشکارسازی وفقی سیگنال های رادار در کلاترگوسی با مدل AR با استفاده از فیلتر کالمن، تهران، مجله علمی پژوهشی رادار
- [۶] ایزدی، محمدقاسم (۱۳۹۰)، روش های اختلال در عملیات شناسایی هوا پایه، تهران، دانشگاه هوافضای عاشورا
- [۷] لطفی، فاطمه و بیغش، مهرزاد و شیخی، عباس (۱۳۹۶)، استفاده از چند آنتن کمکی در کاربرد SLB برای مقابله با جمینگ فریب در رادار جستجوگر، تهران، مجله علمی پژوهشی رادار
- [۸] وایلی، ریچارد (۱۹۹۳)، شناسایی سیگنال های الکترونیکی: تجزیه و تحلیل سیگنال های راداری، ترجمه معاونت فناوری اطلاعات و ارتباطات نهسا، تهران، معاونت فناوری اطلاعات و ارتباطات نهسا
- [9] M.Skolnik, Introduction to radar system, 3rded, c2001
- [10] D. Adamy, EW102, A Second Course in Electronic Warfare, , 2004
- [11] F.Neri, Introduction to Electronic Defense systems, 2nd ed., 2001
- [12] Pace,E.,P. "Detection and Classifying Low Probability of Intercept Radar",Artech