نشریه علمی علوم و فنون نوین هوانوردی
سال ۱ شماره ۲،تابستان ۱۴۰۳

تحلیل پدیده هوانوردی فریب اویونیکی (میجی– MIJI) و ارائه راهکارهای مقابله با آن

نیک بخش حبیبی*[۱] حسن شاه صفی[۲]
۱- دانشیار دانشگاه هوایی علوم و فنون شهید ستاری
۲- استادیار دانشگاه فرماندهی و ستاد
(دریافت مقاله: ۱۴۰۳/۰۳/۱۵تاریخ پذیرش: ۱۴۰۳/۰۴/۲۳)

چکیده

به دلیل استفاده از امواج الکترومغناطیس گسترده در عملیات هوایی این امواج همواره با عملیات الکترونیکی مورد حمله دشمن برای انحراف از بهره برداری در پرواز قرار می گیرند. فریب اویونیکی یا با اصطلاح میجی(MIJI) در زیرمجموعه های حمله الکترونیکی با هدف حمله به فرایندها و ساختارهای الکترونیکی از قبیل حساسه ها، خطوط ارتباطی، شبکه ها به عنوان ابزارهای مشاهده و تصمیم گیری بکار می رود. این نوع از فریب یکی از شگردهای رایج جنگ ناوبری هوایی است که در سطوح تاکتیکی باعث کاهش کارامدی عملیاتی در پرواز شده و مانع استفاده اثر بخش از طیف امواج الکترومغناطیسی می گردد. در این مقاله تلاش شده تا با روش تلفیقی میدانی اسنادی و تجربه پروازی خود نگارنده به عنوان یک هوانورد، روش های شناسایی و مقابله الکترونیکی و عملیاتی با پدیده میجی بیان و راهکارهای برای مقابله با آن نیز ارایه گردید. نتایج حاصل از مطالعه و تحلیل این پدیده نشان می‌دهد که خلبانان و هوانوردان باید قبل از اجرای مأموریت در مناطق خاص و مشکوک، پرونده و سوابق مخاطراتی میجی را مورد مطالعه و بررسی دقیق قرار داده و در مأموریت های ناوبری برای مقابله با این پدیده، ادامه مطمئن پرواز را بر اساس تطبیق عوارض زمین با نقشه قرار داده (ناوبری مستقیم) و در شرایط نامساعد، از دو سامانه مختلف کمک ناوبری و ایستگاه های رادار زمینی استفاده نمایند و هر گونه مورد مشکوکی را از طریق پر کردن فرم (برگ) گزارش مخاطرات پدیده میجی به مراکز عملیات جنگ الکترونیک اعلام نمایند.

کلید واژه ها: الکترونیک هوانوردی ، فریب اویونیکی، میجی، جنگ الکترونیک، تداخل

[۱] * پست الکترونیک نویسنده مسئول: nikbash@gmil.com

مقدمه

ادراکات انسانی و تصمیم‌گیری خلبانان در حین انجام ماموریت همانند هر فرد دیگر می تواند توسط حملات فریب الکترونیکی با هدف ایجاد انحراف، القای اشتباه و خطا، اعمال از هم گسیختگی و پراکندگی به جای یک انسجام روانی و سازماندهی صحیح در حوزه دستگاههای ناوبری و ایونیکی به شدت آسیب پذیر گردد. جنگ الکترونیکی استفاده از طیف الکترومغناطیسی برای کاهش عملکرد، توانایی و یا ممانعت دشمن با هدف حمله به فرایندهای الکترونیکی و ساختار اطلاعاتی از قبیل حساسه ها، خطوط ارتباطی، شبکه ها به کار می روند که می تواند به طور مستقیم بر درک کاربران از شرایط درگیری تأثیر بگذارد (فراتر و ری یان، ۲۰۰۲).

حمله الکترونیکی عبارتست از اقدامی الکترونیکی که به اهداف موجود بر روی یک طیف الکترومغناطیسی حمله می کند. به دلیل استفاده از امواج الکترومغناطیس برای ارتباطات، مخابرات، تشخیص هدف(رادار)، ناوبری و شناسایی این امواج از زمان جنگ جهانی دوم، نخستین محیط مناسب برای جنگ اطلاعات شناخته شده است.

حمله الکترونیکی را می توان در چهار گروه طبقه بندی کرد: بهره برداری، فریب، بازدارندگی یا ممانعت و تخریب(ر.ک به والتز، ۱۹۹۸)

در عملیات فریب مهاجم با کاهش قابلیت های آفندی یا پدافندی رقیب می تواند تأثیر حملات خود را افزایش دهد و در ضمن باعث کاهش اقدامات از سوی او گردد. یکی از انواع مهم عملیات الکترونیکی وقوع پدیده میجی[۱] در فرآیند فریب ناوبری هوایی و اویونیکی یا الکترونیکی هوانوردی[۲] است. که این مقاله درصدد شناخت و نحوه کاهش یا حذف اثرات ناخواسته از این نوع دفاع الکترونیکی به موازات افزایش توانمندی نیروی عملیاتی خودی در فضای یک جنگ اطلاعاتی می باشد.

هدف پژوهش: شناخت ابعاد عملیات الکترونیکی پدیده میجی و ارائه راهکار اثربخش در مقابله با آن در پروازهای مهم و حساس عملیاتی است.

نوع پژوهش: این تحقیق علمی بر اساس هدف از نوع تحقیقات کاربردی است.

روش گردآوری اطلاعات: نگارنده طی عملیات پروازی خود به صورت میدانی در معرض این پدیده قرار داشته و لذا در این تحقیق علاوه بر یافته های میدانی برای جمع‌آوری اطلاعات از روش کتابخانه تخصصی، که در این روش از کتابها و مقالات علمی، آرشیو، سایتهای اطلاعاتی و پیمایش اسناد مرتبط نیز استفاده کرده است. مسأله اصلی و پرسش اساسی تحقیق حاضر بر تحلیل پدیده میجی در فرآیند فریب اویونیکی و راهکارهای مقابله با آن متمرکز است. ضرورت و اهمیت تحقیق در این است که پدیده میجی برای اولین بار در ادبیات علمی نظامی به زبان فارسی توسط یک هوانورد و خلبان شکاری با داشتن تجربه عملیاتی به صورت علمی واکاوی و مورد تحلیل قرار میگیرد. شناخت فرآیند تاثیرگذاری فریب الکترونیکی هوانوردی میجی(MIJI) به دنبال نحوه کاهش یا حذف اثرات ناخواسته این نوع عملیات جنگ الکترونیکی نیز می باشد تا به موازات افزایش توانمندی در عرصه یک جنگ اطلاعاتی، دستاوردهای حاصل از نتایج آن در یک چارچوب نظری معین، زمینه مساعد علمی لازم را برای تصمیم گیری در سطوح عملیات پروازی را فراهم نماید. ضمن آنکه شناخت این پدیده در حوزه دفاع الکترونیکی این امکان را فراهم می سازد تا برای طراحی سامانه های فریب اویونیکی و پادکنش های(ECM) مرتبط با آن اقدام عملی و اثربخش صورت پذیرد.

---

[۱] Meaconing, Intrusion, Jamming, Interference(MIJI

[۲] Avionic Deception

پیشینه موضوع تحقیق

هواپیماهای در حال پرواز در ایران از سه منطقه شمال، غرب و جنوب در معرض جدی فریب الکترونیکی میجی قرار دارد. گزارشات در حین پرواز خلبانان به صورت گزارش شفاهی به نگارنده و کتبی در این سه منطقه نشان می‌دهد که پرواز در این مناطق با ریسک این نوع از محدوده فریب اویونیکی روبرو است. بارها در پرواز در ناحیه شمال و غرب نگارنده با اختلال تداخل ناوبری[۱] به ویژ در ناحیه شمال(۱۳۷۳ شمسی یا ۱۹۹۴ میلادی) و با اخلال رادیویی[۲] در ناحیه غرب روبرو شدند. همکاران عملیاتی نیز مشابه همین اخلال را در ناحیه جنوب به کرات مشاهده کردند. نمونه گزارش این اخلال را در تصویر ۱ طی سال‌های جنگ تحمیلی عراق علیه ایران (نهم مهرماه ۱۳۵۹ شمسی) می‌توان مشاهده کرد. اول سپتامبر ۱۹۸۳ پرواز ۰۰۷ خطوط هوایی کره از نیویورک به سئول در حالی که از مسیر اولیه خود منحرف شده بود توسط هواپیماهای شکاری روسی(شوروی سابق) به بهانه پرواز بر روی مناطق ممنوع رهگیری و منهدم شد. در این سانحه هوایی همه ۲۶۹ مسافر و خدمه پرواز کشته شدند. یکی از فرضیه‌های مطرح شده انحراف به دلیل تداخل ناوبری برای انحراف عمدی و سپس انهدام هواپیمای مسافربری به دلیل وجود سناتور حزب دمکرات «لری مک دونالد[۳]» رهبر مخالفان کمونیسم در کنگره در این پرواز بوده است[۴]

۱۰ آوریل ۲۰۱۰، هواپیمای توپولوف ۱۵۴ نیروی هوایی لهستان در نزدیک فرودگاه شهر اسمولنسک در غرب روسیه سقوط کرد که نود و شش سرنشین آن از جمله « لخ آلکساندر کاچینسکی»، رئیس جمهوری لهستان و همسرش به همراه چند عضو بلندپایه دولت، ارتش و مجلس این کشور کشته شدند. این هیات بلندپایه لهستانی به منظور شرکت در مراسم هفتادمین سالگرد کشتار کاتین(پاییز ۱۹۴۳) به دستور نیروهای امنیتی استالین در حال سفر به روسیه بودند. این هواپیما از ورشو به مقصد فرودگاه اسمولنسک، در نزدیکی مرز روسیه با بلاروس در حال پرواز بود که سقوط کرد. دلیل سقوط هواپیمای توپولوف ۱۵۴ لهستان امتناع خلبان از فرود در باند اضطراری بوده در زمانی که او اخبار و گزارش مبنی بر بارش برف و شرایط نامناسب باند فرودگاه تعیین شده برای فرود را دریافت کرده بود. تحقیقات اولیه با همکاری دولت لهستان و روسیه نشان داد که مه غلیظ باعث کاهش دید خلبان و خطای او و در نتیجه سقوط هواپیما شده بود، رئیس جمهوری لهستان پس از سالها قرار بود در راه نزدیکی کشور خود با روس‌ها قدم‌های جدی بردارد. ولی فرض تداخل ناوبری و وادار کردن خلبان به اشتباه از سوی منبعی ناشناخته در مرز بلاروس یکی از فرضیه‌های جدی سانحه به شمار می‌رود[۵] دسامبر ۲۰۱۱ (۱۳ آبان ماه ۳۹۰ شمسی) نیروهای مسلح ایران موفق شدند با فریب ناوبری و دستکاری اطلاعات مرتبط با ارتفاع سنج[۶] پهپاد ار کیو ۱۷۰ معروف به سنتینل را به غنیمت بگیرند. البته مقامات آمریکایی نقص در سیستم موقعیت یاب جهانی هواگرد فوق را علت سقوط اعلام کرده‌اند. در هر حال آن چه که اتفاق افتاد ناشی از اختلال ناوبری بوده است.

---

[۱] Meaconing

[۲] Intrusion

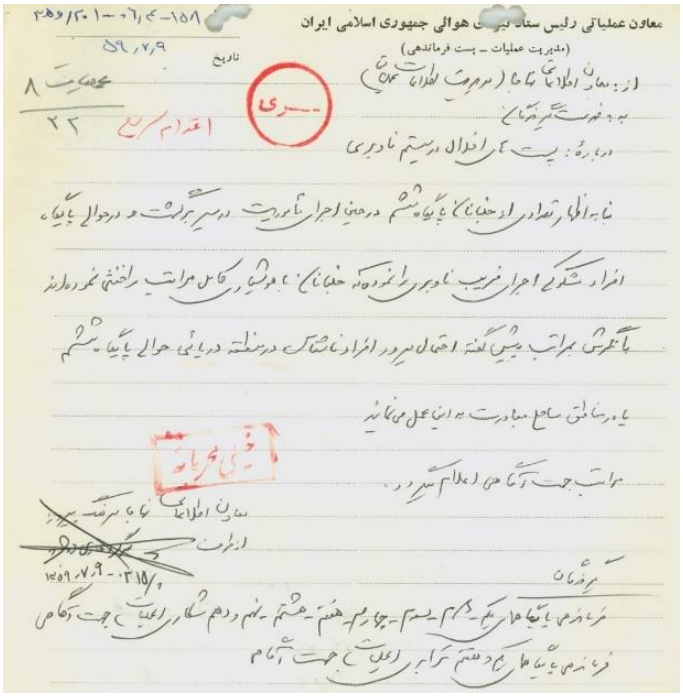
[۳] Larry McDonald

[۴] https://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_۰۰۷_alternative_theories#Meaconing

[۵] https://en.wikipedia.org/wiki/Meaconing

[۶] false altitude measurements

تصویر – ۱ نمونه گزارش اخلال ناوبری طی جنگ ایران و عراق در مهرماه ۱۳۵۹ شمسی



بحث و بررسی

جنگ و فناوری اطلاعات

توسعه زیرساختهای فناوری مقدمه و جواز ورود به دنیای سوم یا عصر دانش پایه یا اطلاعات محور است. تکنولوژی هوانوردی مهمترین نقش را در انتقال جنگ از حوزه تسلیحات فیزیکی به حوزه فرایندهای اطلاعاتی و دانشی ایفا می کند. این امر همان چیزی ست که از ابتدای دهه هشتاد میلادی در ذیل موج سوم تولید ثروت مبتنی بر مالکیت اطلاعات توسط تافلر بیان شد. (تافلر، ۱۹۸۰)

با گذشت زمان ، فناوری الکترونیک نقش بسزایی را در عملیات های هوایی به عهده داشته و مراحل مختلفی را پشت سر نهاده است . تاریخ و نخستین مرحله آن به زمان اختراع هواپیما بر می گردد. امروزه تقریباً کلیّه پرنده ها و هواگردها، سامانه های اویونیکی ارتباطی، مخابراتی، ناوبری و شناسایی الکترونیکی را به کار گرفته اند. حمله به این سیستم های اویونیکی به قصد انحراف، تخریب، اختلال و فریب الکترونیکی آسیب جدی به عملکرد و کارآیی هواپیماها و کادر پروازی وارد خواهد ساخت. محققان برای هر جنگی چهارحوزه مشخص قائلند. این چهار حوزه به طور خلاصه عبارتند از فیزیکی، ادراکی، شناختی و اطلاعاتی. (والتز، ۱۹۹۸)

این حوزه های چهار گانه، برای اولین بار به طور سیستماتیک و یکپارچه تحت تأثیر تکنولوژی نظامی جنگ اطلاعات در جنگ اول خلیج فارس نیروهای ائتلاف علیه عراق در سال ۱۹۹۱ با عملیات فیزیکی، روانی، فریب و الکترونیک مورد حمله قرار گرفت. اصطلاح جنگ اطلاعات توسط اندیشمندانی چون تام رونا، الوین تافلر، الن کمپین، و وین شوارتا در صدر جنگهای پست مدرن قرار گرفت. حوزه ادراکی، یک فاکتور انسانی ست که به جدیت انسانهای تصمیم گیر و تمایل ارادی آنها به اقدامات مختلف در جنگ بستگی دارد. این حوزه از مبهم ترین پارامترها برای اندازه گیری، مدل کردن و تأثیر گذاری مستقیم برخوردار است. حوزه شناخت، یک فاکتور اطلاعاتی ست که تابع درک و دیدن شرایط از دیدگاه طرف متخاصم می باشد که می تواند با پارامترهای از قبیل دقت ، درجه اطمینان یا ابهام و سرعت عمل در واحد زمان قابل اندازه گیری شود .

کلیه تصمیماتی که دشمن اتخاذ می کند بستگی به نحوه درک شرایط ایجاد شده از سوی ما و برداشتهای او از ظرفیت های خود دارد. این اصل شناختی در همه جنگ ها وجود دارد که همواره بر مبنای فهم از شرایط موجود و درک اقدامات مختلف و نتایج متحمل آنها و میزان تمایل تصمیم گیران طرف متخاصم در جنگ اقدامات خود را عملی می کند. (جانسون و همکاران۲۰۰۳)، همواره هدف اطلاعات را تأثیرگذاری بر تصمیمات دانسته تا آنجا که معتقدند هدفی جز این، اطلاعات را ابزاری برای سرگرمی و خود اشتغالی درمی‌آورد. در گذشته کلیه تصمیمات تا قبل از جنگ جهانی دوم توسط افراد اتخاذ می شد ولی با پیشرفت سیستم های اطلاعاتی دیجیتالی بخش گسترده ای از این تصمیمات و گزینه های انتخاب شده از بین یک سلسله از اقدامات و کارهای مختلف توسط ماشینها که جزیی از تکنولوژی جنگ بشمار می روند، اتخاذ می شوند، بنابراین چنین فرض می‌شود که اگر بتوان به هر عاملی که در ورودی اطلاعات به چرخه تصمیم گیری در تکنولوژی سخت و ماشین ها و ابزارهای بکارگرفته شده تأثیرگذار شد می توان در نتایج حاصل از تصمیم گیری دخالت کند و جنگ اطلاعات نتیجه چنین تأثیر گذاری در صحنه عملیات به شمار می رود. جنگ اطلاعات به سلسله اقداماتی اطلاق می‌شود که برای تأثیر گذاری بر فرآیند تصمیم گیری دشمن صورت می گیرد به طوریکه تصمیمات دشمن بد یا با تأخیر یا به نفع شما صورت گیرد (مثل ترک مخاصمه به جای جنگیدن). به همین دلیل است که تکنولوژی به عنوان پایه نفوذ به چارچوب عملیاتی جنگ اطلاعات به شمار می‌رود، هم از حیث ابزار تکنولوژی سخت و هم از حیث تصمیم گیری نهایی که به شدت تحت تأثیر حوزه تکنولوژی نرم می‌باشد. نقطه ورودی جنگ اطلاعات، جمع آوری اطلاعات سیگنالی به کمک حسگرهاست. برای اختلال در امر حسگرها می توان به یکی از سه راه زیر متوسل شد یا آنها را منهدم کرد یا آنها را فریب داد و یا اینکه با پنهانکاری آنها را مخفی کرد. همانطور که مشاهده می شود در هر سه حالت نیازمند نوعی خاص از تکنولوژی هستیم که بدون آنها این امر اختلال حسگرها امکان پذیر نیست. در جنگ اطلاعات یا خود پدیده و سوژه مورد نظر را دستکاری می کنند تا مشاهده کنند به اشتباه بیفتد و این با فریب مسیر است. (هندسه فراکتال در پدافند غیر عامل می تواند چنین نقشی را ایفا کند) . این جنگ در حوزه ادراک است. یا چارچوب ذهنی و ادراکی مشاهده کننده را به نحوی مورد تأثیر قرار می دهند که او حتی با مشاهده اصل موضوع نتایج اشتباه اتخاذ کند به عبارت دیگر او تحت تأثیر عملیات روانی و حتی اراده و تمایل خود را تحت تأثیر آنچه که او می خواهد در می آورد این جنگ منشاء جنگ شناختی است. و یا اینکه اطلاعات حاصل از دریافت و ارسال سیگنالها توسط حسگرها و حساسه ها یا اقدامات تداخلی یا تخریبی یا انحرافی مورد حمله قرار می گیرد که به آن جنگ الکترونیک گفته می شود (والتز، ۱۹۹۸).

حوزه اطلاعاتی، قلمرو الکترونیکی ست که طرف متخاصم توسط آن محیط خود و صحنه جنگ یا رقیب را مشاهده می کند ، می تواند حملات رقیب را نظارت یا کنترل کند، شرایط نیروهای خودی را ارزیابی و گزارش های حاصل از محیط اطراف را مخابره کند همانطورکه اشاره شد، هر چهار حوزه (فیزیکی، ادراکی، شناختی و اطلاعاتی) می تواند به ترتیب توسط حمله فیزیکی، عملیات روانی، نبرد شناختی و حمله اطلاعاتی الکترونیکی آسیب پذیر شوند. ظرفیت های فیزیکی عبارتند از: تسلیحات نظامی نیروها، قرارگاه ها و پایگاه های نظامی، ظرفیت های صنعتی، پل ها و منابع حیاتی دیگر، گروه های فرماندهی و کنترل و... هدف مهم فیزیکی تخریب این ظرفیت هاست. هدف نهایی جنگ الکترونیک، تقلیل کارائی و تأثیرات سیستم های است که از حسّاسه های الکترونیکی در عملیات خود بهره می جویند. مزایای کاربرد تکنیک های ضد الکترونیکی زیاد است و این تکنیک ها به جایی رسیده اند که می توانند بطور جدّی، کارایی و عملکرد اکثر سامانه های هوایی و هواپیماها و حتی سامانه های زمین پایه و دریا پایه را نیز به شدت کاهش دهند. در جنگ های امروزی، فرماندهی که مقدورات و امکانات جنگ الکترونیکی به او اجازه صدور دستور ندهد و نگذارد از تجهیزات خود به نحو مطلوب بهره برداری نماید و جلوی ترتیبات لجستیکی، آمادی و اداری اورا بگیرند با هر استعدادی محکوم به شکست است. امروزه توان جنگ الکترونیک عملیاتی، سخت افزاری و نرم افزاری، بخشی از توان رزمی نیروهای مسلّح محسوب می گردد(ستاری‌خواه،۱۳۸۶).

جنگ الکترونیکی، بکارگیری انواع سامانه های سخت افزاری، نرم افزاری ارتباطاتی اطلاعاتی و عملیاتی در جنگ افزارهای آفندی و پدافندی نیروهای مسلّح، به عنوان یک اقدام پشتیبانی عملیات های رزمی، جهت دستیابی به اقتدار رزمی در یک نبرد واقعی است .جهت دستیابی به چنین منظوری، اقدامات ذیل الزامی است:

الف- داشتن اطلاعات استراتژیکی و تاکتیکی از تجهیزات وفناوری الکترونیکی دشمن

ب- انجام اقدامات ضد الکترونیکی[۱] یا پادکنشی(ECM) تهاجم الکترونیکی: هدف از انجام این اقدامات کاهش هر چه بیشتر مقدورات الکترونیکی سیستم های دشمن اعم از راداری، تجسّسی، اکتسابی و تعقیب کننده، سیستم های مادون قرمز، لیزری و ارتباطی می باشد. وظیفه " اقدامات ضد الکترونیکی" خنثی سازی سامانه های الکترونیکی کشف شدهٔ دشمن است. هدف سامانه های تهاجم الکترونیکی (اقدامات ضد الکترونیکی) انحراف، تخریب، ممانعت و فریب دادن سامانه ها و حسّاسه های الکترونیکیِ دشمن است.

د- انجام اقدامات ضدالکترونیکی[۲] یا ضدپادکنشی(ECCM) حفاظت الکترونیکی: در حقیقت گاهی اوقات این امکان وجود دارد که حمله الکترونیکی اخلال و یا تداخل عمدی دشمن را با بهره گیری از فیلترها و دیگر تجهیزات ضد جنگ الکترونیک کاهش داد ویا حذف نمود. تجهیزات سخت افزاری ونرم افزاری ضدضد الکترونیکی معمولاً به حسّاسه های انواع جنگ افزارهای نیروهای مسلّح (پدافندی، اطلاعاتی و...) اضافه می شوند تا آنها را قادر سازند که در محیط الکترونیکی دشمن، یعنی در حضور پارازیت رسان عمدی، با به حداقل کاهش دادن توانائی های معمولی آنها، فعالیّت کنند. چنین اقداماتی، تدافع الکترونیکی یا اقدامات ضدضد الکترونیکی نامیده می شود. برای انجام اقدامات ضدضد الکترونیکی باید این عملیات ها صورت پذیرد :

۱- اقدامات بازدارنده، که شامل استفاده از توان پایین دستگاهها و استفاده نکردن یکنواخت از دستگاهها می باشد.

۲- اقدامات بازدارنده ضدضد الکترونیکی، که شامل دقت در انجام عملیات با توجه به فناوریهای جایگزین و فرعی و جلوگیری از جمع آوری اطلاعات توسط دشمن است.

۳- اقدامات اصلاحی، که در هنگام اختلال دشمن قابل اِعمال است(همان مدرک).

جنگ ناوبری هوایی

جنگ ناوبری هوایی می تواند مثل هر عملیاتی از نوع جنگ الکترونیک به سه وجه حمله الکترونیکی، حفاظت یا دفاع الکترونیکی و پشتیبانی الکترونیکی تقسیم گردد.(ر.ک به فراتر و ری یان، ۲۰۰۲،) (جدول ۱)

جنگ ناوبری یکی از انواع جنگ الکترونیک است که به سامانه ناوبری، الکترونیک هوایی و یا سامانه تعیین موقعیت جهانی (GPS) با این هدف حمله می کند که دشمن را از داشتن اطلاعات ناوبری، الکترونیکی، به موقع و دقیق بازداشته و همزمان اطلاعات ناوبری و الکترونیکی دقیق را برای نیروهای خودی ایجاد نماید.

---

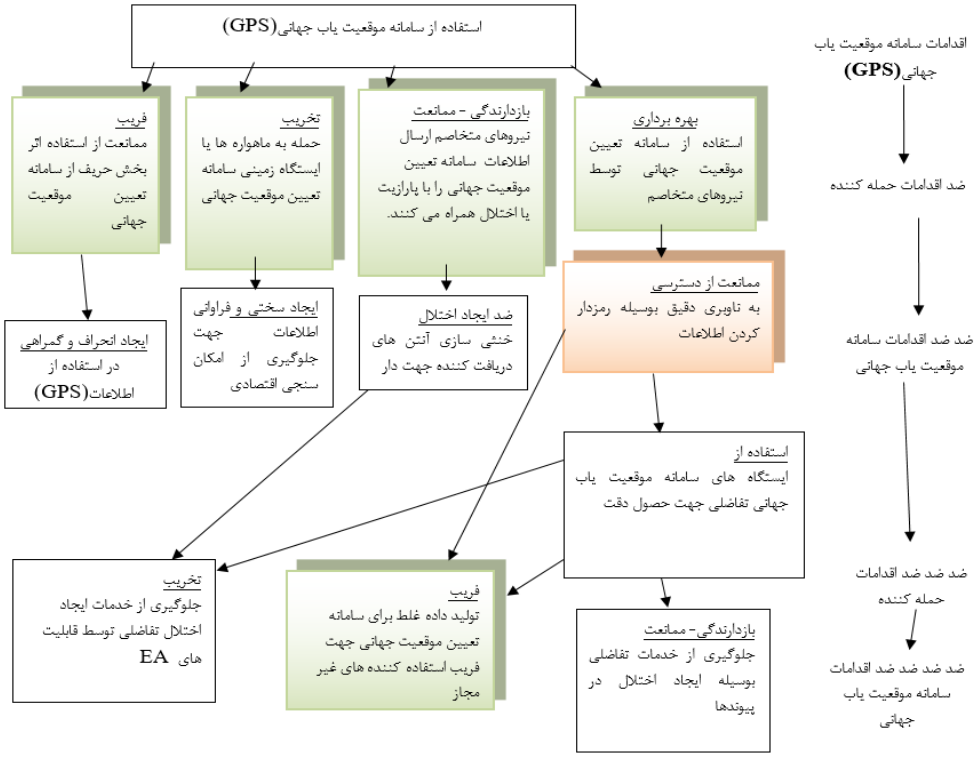
[۱] Electronic Countermeasures

[۲] Measures Electronic Counter-Counter

بخش های جنگ ناوبری هوایی	عملکرد	کاربرد
حمله الکترونیکی(EA)	استفادهاز الکترومغناطیس یا انرژی هدایت‌شده برای تخریب، اختلال و انحراف سامانه های اویونیکی و گمراهی عوامل انسانی	انرژی هدایت شده RF یا انرژی لیزری علیه سامانه های‌راداری،مخابراتی، ناوبری و سایر سامانه هایی که امواج الکترومغناطیس را دریافت و یا منتشر می کنند.
حفاظت الکترونیکی (EP)	فعالیت‌هایکه‌برای‌حفاظت ازنیروها، تأسیسات‌وتجهیزات‌سامانه های اویونیکی انجام می شود.	دریافت‌امواج جهت تشخیص نوع اختلالات، یا حفاظت علیه انرژی هدایت شده. ایجاد اختلال با حفاظت از سامانه های خودی چف RFیاشراره‌الکترواپتیکی (EO)به‌عنوان‌هدف‌مصنوعی.
حمایت الکترونیکی (ES)	فعالیت های ابلاغ شده یا تحت کنترل مستقیم یک فرماندهعملیات،جهت‌جستجو برای.رهگیری،تشخیص‌و یافتن منابع انتشار انرژی الکترومغناطیس با هدف و بی هدف	تشخیص تهدید و رفع تهدید اتخاذ تصمیم های عملیات جنگ الکترونیکی‌یا حفاظت الکترونیکی آنی جمع آوری اطلاعات برای هدف گیری فعالیت های تاکتیکی

به عنوان مثال، اتکاء عام (سامانه های اویونیکی نظامی و غیر نظامی) به سامانه تعیین موقعیت جهانی(GPS) در سال های اخیر باعث شده سامانه هایی برای مقابله با آن و اقدام متقابل طراحی شوند، به نحوی که مانع دسترسی یک شخص یا یک منطقه به اطلاعات دقیق ناوبری گردد. آسیب پذیری ناوبری توسط سامانه تعیین موقعیت جهانی ناشی از نفوذ پذیری سیگنال دریافتی (باند فرکانس L۱ در ۱۵۷۵/۴۲ مگاهرتز تقریبا ۱۶۰ دسیبل وات را در سطح زمین انتقال می دهد و باند فرکانس L۲ در ۱۲۲۷/۶ مگاهرتز، ۱۶۶ دسیبل وات را منتقل می کند) است که شرایط بازدارندگی یا حذف سیگنال را فراهم می آورد. در شکل۱ تسلسلی از اقدامات (M)، ضد اقدامات یا پادکنشی (CM) وضد ضد اقدامات یا ضدپادکنشی (CCM) که در جنگ ناوبری علیه سامانه تعیین موقعیت جهانی اعمال می شود، به صورت خلاصه نشان داده شده است. توجه داشته باشید که هر یک از عملیات اصلی جنگ الکترونیک توسط هر دو طرف مهاجم و مدافع سامانه موقعیت یاب جهانی مورد استفاده قرار می گیرد، یعنی عملیات بهره برداری، ممانعت، فریب، تخریب. این ساختار تنها یک نمونه است و تمامی عملیات ممکن و قابل تصور را شامل نمی شود. عملیاتی مانند تغییر در سیگنال های مستقیم و اعمال تفاضل در سامانه موقعیت یاب جهانی که باعث می شود تا قربانی مورد هدف، داده های ناوبری اشتباهی را دریافت کند (والتز ، ۱۹۹۸).

شکل – ۱ توالی اقدامات اساسی در یک جنگ ناوبری هوایی مرتبط با سامانه موقعیت یاب جهانی(GPS)
منبع : (والتز ، ۱۹۹۸)

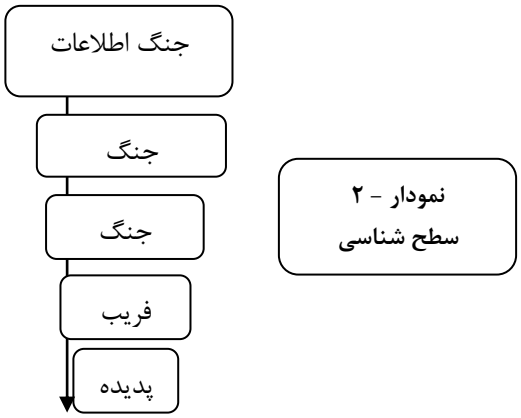


جدول – ۲ طبقه بندی کلی حملات الکترونیکی
منبع : (والتز ، ۱۹۹)

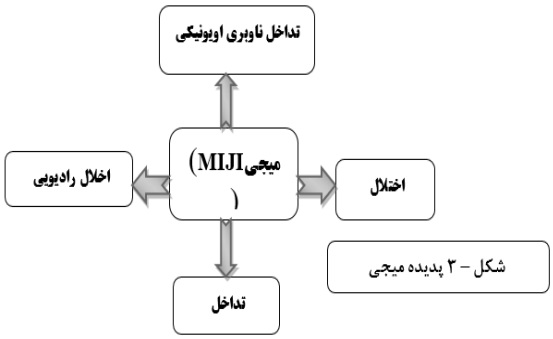
طبقه بندی	فعالیت عملی	روش های قابل ارائه	سیستم های قابل ارائه
بهره برداری	استخراج اطلاعات از حساسه ها یا سامانه ارتباطاتی طرف مقابل و بهره برداری از دانش کسب شده جهت فریب ، ممانعت ، براندازی یا تخریب	سامانه راداری دریافت اخطار (RWR) اقدامات‌حمایت الکترونیکی (ESM)	رهگیری راداری (ELINT) برای حمله به هدف گیری (بازدارندگی ، ممانعت ، یا نابودی) رهگیری مخابراتی (COMINT) رهگیری شبکه ای
فریب	وارد کردن اطلاعات غلط به درون حساسه ها یا سامانه های ارتباطاتی طرف مقابل	سیگنال های فریبنده پیام های غلط حضور مجازی یا خود را بعنوان خودی جا زدن	فریب راداری جهت حذف اهداف، داخل کردن اهداف اشتباه وارد کردن پیام ها یا همزمان سازی غلط ارتباطاتی
بازدارندگی یا ممانعت	کاهش کارایی اطلاعاتی (مثلا کاهش توان دریافت ،، دقت ، تجسس ، نرخ ردیابی ، تشخیص و شناسایی ، ظرفیت ، حداکثر ورودی و افزایش نرخ خطا) در حساسه ها یا سامانه های ارتباطاتی طرف مقابل	ایجاد اختلال یا پارازیت (انواع‌مختلف):باندوسیع،جاروب،واکنشی، دنبال‌کردن،پیوسته، دنبال گشتن، تکرار سیگنال و اشباع	ایجاد اختلال راداری ایجاد اختلال ارتباطاتی تاخیر ارتباطاتی و تکرار
تخریب	از میان بردن توانایی جمع آوری، پردازش، یاتوزیع اطلاعات حساسه‌یاسامانه ارتباطاتی طرف مقابل	حذف ملایم:دفع موقتی یا عملکردی ، احتمالا غیر فیزیکی حذف شدید: دفع دائمی یا فیزیکی	موشک ضد تشعشع انرژی هدایت شده : انرژی فرکانس رادیویی انرژی لیزری

پدیده میجی(چالش ها و راهکارها)

پدیده میجی(MIJI) نوعی فریب اویونیکی یا الکترونیک هوانوردی است که خود نوعی عملیات الکترونیکی به شمار می رود. که جزئی از عملیات جنگ ناوبری هوایی یک جنگ الکترونیک از زیر شاخه های جنگ اطلاعات می باشد.(شکل۲)



پدیده میجی نوعی ایجاد فریب الکترونیک هوانوردی یا اویونیکی در حساسه های الکترونیکی سامانه های اویونیکی و کاربران انسانی این سامانه ها به منظور ایجاد تاثیر ادراکی، شناختی و اطلاعاتی است. میجی(MIJI)، واژه به اختصار درآورده چهار واژه مرتبط با حمله الکترونیکی تداخل ناوبری[۱]، اخلال رادیویی،[۲] اختلال[۳] و تداخل[۴] می‌باشد. (شکل -۳)



فریب اویونیکی، یک پدیده الکترونیکی در سامانه‌های اویونیک به هنگام بهره برداری در پرواز است. این پدیده مانع استفاده اثر بخش دشمن از طیف امواج الکترومغناطیسی می گردد، که در ادبیات جنگ اطلاعات و زیر مجموعه آن یعنی جنگ الکترونیک به آن پدیده میجی[۵] (MIJI) گفته می شود.

رد و بدل کردن اطلاعات در قالب یک جنگ ناوبری در حین پرواز چیزی شبیه عملیات فریب رایانه ای است که به صورت مجازی نیز می تواند اتفاق بیفتد. والتز(۱۹۹۸) این موضوع را به صورت زیر در ذکر نمونه ای اینگونه بیان می کند:

"فریب با مقاصد خصمانه جهت وادار کردن افراد در تهیه نمودن اطلاعات برروی اینترنت نیز بکار گرفته می شود، در حالیکه آنها فکر می کنند بطور امن در حال محاوره بر روی " شبکه وب جهانی " می باشند. یکی از انواع این نوع فریب

---

[۱] Meaconing

[۲] Intrusion

[۳] Interference

[۴] Interference

[۵] Meaconing, Intrusion, Jamming, Interference(MIJI)

"حضور مجازی در وب" نام دارد که از عملیات فریب گمراه کننده استفاده می کند و قبل از هر چیز همانند یک قربانی در یک پایگاه اینترنتی با وضعیت "حضور مجازی" به دام می افتد .
پایگاه اینترنتی "حضور مجازی" در واقع نقش یک واسط را ایفا می کند. به این صورت که آدرس اینترنتی (URL) را بر روی صفحه وب "حضور مجازی" باز نویسی می کند و به طرف سرور مهاجم بر می گرداند. سرورهای مهاجم سایه ای از کل "شبکه وب جهانی" ایجاد می کند که در آن کلیه درخواست های مرورگر قربانی به طرف سرور مهاجم فرستاده می شود و این سرور، صفحه درخواست شده (قانونی) را بدست می آورد و کلیه پیوندهای مربوطه را به سرور مهاجم می فرستد. همین که قربانی اسیر گردد، رایانه سرویس دهنده مهاجم کلیه مبادلات اطلاعاتی وی را می تواند مشاهده کند و این موضوع می تواند شامل برملا شدن کلمه رمز عبور، شماره حساب ها و یا دیگر داده های محافظت شده نیز باشد."
پیشرفت عملیات اطلاعاتی مبتنی بر فناوری های پایه ای است که عملکرد آنها به سرعت در حال تغییر است. با توجه به اینکه فناوری های جدید توانایی آفند و پدافند پیشرفته تری را ایجاد کرده اند به نظر می رسد فناوریهای نوظهور بتوانند افق های کاملا" جدیدی را برای جنگ اطلاعات ترسیم کنند.
پدیده میجی، یکی از شگردهای رایج جنگ ناوبری هوایی است که در سطوح تاکتیکی باعث کاهش کارامدی عملیاتی در پرواز می گردد. بررسی گزارش های خلبانان و کاربران ارتباطات هوایی نشانگر بعضی از موارد اختلال عمدی در سامانه‌های ارتباطی ناوبری هواپیماها می باشد و چون این اختلالات بیشتر در مناطق خاصی صورت می گیرد چنین استنباط می شود که این عمل ناشی از عملیات فریب ناوبری هوایی می باشد.
روش های شناسایی و مقابله با پدیده میجی در عملیات فریب ناوبری به دلیل آسیب پذیری سامانه‌های الکترونیکی هواپیما در برابر این گونه عملیات بسیار مهم و حایز اهمیت است. باید در روند اجرای عملیات هوایی اطمینان حاصل کرد که با اجرای دقیق فرآیند مقابله با عملیات فریب ناوبری تاثیر آن را بر روند ادامه پرواز عاری از دخالت و فریب ساخت.
در ابتدا به تقسیم بندی رایج و شناخته شده و چالش های پدیده میجی می‌پردازیم و سپس به ارایه راهکارهای مقابله با آن اشاره می کنیم:

الف : تداخل ناوبری(Meaconing)

فرآیندی است که با استفاده از یک سامانه، علایم رادیویی دستگاه های ناوبری را دریافت و سپس با تقویت بیشتر روی همان فرکانس باز انتشار یا ارسال مجدد می کند و سبب گمگشتگی، اختلال و انحراف سامانه ناوبری هواپیمای خودی شود. این امر باعث می شود تا هواپیماها از مسیر خود منحرف و هدف را از دست بدهند. نصب دستگاه های ناوبری مشابه دستگاه های خودی از قبیل تکن و رادیو بیکن و... با قدرت انتشار سیگنالهای قوی تر در مجاورت مناطق عملیاتی مورد نظر باعث می گردد که دستگاه های ناوبری هواپیما در مقابل آنها عکس العمل مثبت نشان داده و بجای نشانه روی به طرف ایستگاه (اصلی) به سمت آنها منحرف گردد، این عمل گذشته از گمراه کردن(خدمه پروازی) در امور ناوبری، باعث می گردد که اکثر هواپیما ها به مناطق پدافند هوایی دشمن هدایت شده و در معرض مخاطرات جدی قرار گیرند. اثرات عمده ای که تداخل ناوبری در یک صحنه عملیات به همراه دارد، عبارتند از:

۱: انحراف و هدایت هواپیما به فضای عملکرد و قدرت آتش یا منطقه نشستن اجباری دشمن
۲: انحراف از مسیر پروازی مورد نظر
۳: انهدام اهداف غیرواقعی
۴: اشتباه دستگاه های زمینی در دریافت موقعیت و مختصات مکانی پرنده ها

ب : اخلال رادیویی (Intrusion)

تداخل عمومی رادیویی با ارسال امواج الکترومغناطیس رادیویی در مسیر ارسال و دریافت امواج رادیویی به منظور دادن اطلاعات اضافی، غلط، هدایت یا گمراهی، ارائه اهداف موهوم، هماهنگی آتش بی موقع، یا حتی باز تکرار یا باز پخش اطلاعات غلط.روش هایی که صداها را نسخه برداری می کند (از طریق استراق سمع، تغییر و ارسال دوباره) و آنها را برای فریب کاربران سامانه های رادیویی مورد استفاده قرار می دهد. اصطلاحات گفتاری به شکل دگرگونی در نوع کلمات ("تغییر شکل کلمات") در تصاویر ویدیویی نیز به طور مشابه می تواند، جهت ایجاد اطلاعات ویدیویی فریب دهنده مورد استفاده قرار گیرد. (والتز، ۱۹۹۸)

در این نوع عملیات، دشمن سعی می نماید که اطلاعات غلط و یا سمت و مسافت اشتباه، را روی فرکانس رادیویی که خدمه پروازی به گوش هستند ارسال نماید و احتمالاً آنها را از ادامه مأموریت باز داشته و یا به سوی نقطه دیگری بکشاند و حتی الامکان کوشش می کند که پیام های ارسالی به زبان محلی و نحوه مکالمه شبیه کنترلرهای خودی باشد.

پ: اختلال (Jamming)

انتشار امواج انرژی دار الکترومغناطیسی، جهت ممانعت و جلوگیری از عملکرد جاری تجهیزات و سامانه های الکترونیکی. دشمن در این اقدام استفاده مؤثر ما را از با ایجاد پارازیت و اختلال در دستگاه‌های ارتباطی، سامانه‌های کنترل آتش، سامانه های راداری، دستگاه های ناوبری، ماهواره و الکترو اپتیک، دچار اختلال و ناکارآمدی می کند. ایجاد اختلال در دستگاه های ارتباطی، ناوبری، و سامانه کنترل آتش هواپیما، یکی از متداول ترین و موثرترین تکنیک های فریب ناوبری می باشد. تأثیر این نوع فعالیت های الکترونیکی بر سامانه‌های فوق به حدی است که حتی در بعضی موارد انجام مأموریت را غیر ممکن می سازد.

ت: تداخل (Interference)

تداخل به هر مزاحمت یا اخلال الکترونیکی می گویند که سبب پاسخ های نامطلوب و غیر دلخواه در سامانه ها و تجهیزات الکترونیکی نظیر رادیویی، راداری، دستگاه های ناوبری، ماهواره ای و الکترواپتیکی می شوند. این تداخل می تواند در منطقه خودی، دشمن و فضای کل نبرد و یا حتی اخلال در پخش یا دریافت امواج رادیویی کشوری نیز گردد.

تهیه روش یکنواخت جهت مقابله، گزارش، تجزیه و تحلیل فعالیتهای فریب ناوبری و تعیین محل احتمالی وقوع این نوع از فریب الکترونیکی از حساسیت ویژه ای برخوردار است. گزارش میجی[۱] سندی ست که همه موارد قطع امواج رادیویی، راداری، کمک های ناوبری، ماهواره ای و الکترواپتیک را گزارش می کند. این گزارش دو کمک اساسی به حوزه مرکز فرماندهی و کنترل هوایی می کند. یکی اینکه اطلاعاتی را در خصوص مشکل میجی به فرمانده تاکتیکی هوایی می دهد تا با در نظر گرفتن آن چاره ای برای حل آن از لحاظ تاکتیکی یا عملیاتی بنماید. دوم آنکه سابقه ای از رویداد میجی را ثبت می کند تا در فضای عملیات ضد الکترونیکی[۲] چاره ای برای غلبه بر آن به کمک مهندسین و گروه متخصصین فنی جنگ الکترونیک بیندیشند و یا اتخاذ نمایند.[۳]

---

[۱] MIJI Report

[۲] ECCM

[۳] ص ۱-۴ FM۲U ر.ک به ۳۳-

راهکارهای مقابله با فریب ناوبری (میجی)

۱- تکنیک انسانی

الف : تداخل ناوبری

در صورت مشاهده این نوع فعالیت با در نظر گرفتن شرایط جوی خدمه پروازی به ترتیب زیر عمل نمایند:

(۱) پرواز V.F.R یا همان پرواز در شرایط دید مناسب[۱]، خدمه پروازی در چنین حالتی بلافاصله باید از نقشه و نقطه نشانه های زمینی به منظور ناوبری مستقیم[۲] و سایر دستگاههای کمک ناوبری موجود در هواپیما به منظور تشخیص موقعیت خود و پرواز در مسیر مطمئن استفاده نمایند.

(۲) در پرواز I.F.R یا همان پرواز در شرایط بدون دید[۳]، خدمه پروازی باید از کنترولر رادار زمینی کمک خواسته و موقعیت خود را با او مطابقت دهند و یا اینکه از سایر هواپیما هایی که در حال پرواز در مناطق مجاور هستند کمک گرفته وضمن استفاده از کلیه دستگاه های کمک ناوبری موجود در هواپیما، موقعیت خود را مشخص نمایند.

ب : اخلال رادیویی

به منظور مقابله با این تکنیک خدمه پروازی می‌توانند با تغییر فرکانس های رادیویی و بهره گیری از دستگاه های کمک ناوبری از صحت پیام ها ی ارسالی و همچنین موقعیت خود آگاه شوند.

پ: اختلال

به علت وجود اختلالات بسیار پر قدرت برروی سامانه های مختلف الکترونیکی هواپیما مقابله با این عملیات بدون داشتن سامانه های ضد الکترونیکی دشوار و حتی در بعضی موارد غیر ممکن میباشد.

روش های زیر به منظور کاستن اثرات این نوع عملیات فریب لازم خواهد بود:

(۱) در صورتی که عمل اختلال روی فرکانسهای ارتباطی انجام گیرد با انتخاب آنتن مناسب تغییر آن از حالت آنتن پایین[۴] به آنتن بالا[۵]و بلعکس و با تغییر بسامدهای (فرکانس های) رادیویی و بالا و پایین نمودن صدای رادیو باید سعی شود حتی الامکان مکالمه را قابل تشخیص نموده و همچنین خدمه پروازی آمادگی داشته باشند که اگر در دسته های چند فروندی پرواز می نمایند مکالمات رادیویی را به حداقل رسانیده و سکوت رادیویی را مراعات نمایند و ضمناً مطالب ضروری را با استفاده از علایم قرار دادی بصری به اطلاع یکدیگر برسانند.

(۲) اگر عمل اختلال روی دستگاه های کمک ناوبری صورت گیرد، چون این دستگاه های در فرکانس های مختلف کار می کنند اگر محل یک و یا قسمتی از آنها مختل ویا متوقف می شود باید با استفاده از سایر وسایل کمک ناوبری و همچنین بهره گیری از راهنمایی های کنترلر رادار زمینی موقعیت خود را مشخص نمود.

(۳) اختلالات تولید شده از عمل اختلال بر روی سامانه ها و بمباران هوشمند هواپیما۶ قابل رویت نبوده و فقط نتایج حاصل از بمباران میتواند اثرات این نوع فعالیت را نشان دهد که در این صورت بهترین طریقه پرتاب بمب با استفاده از روش مستقیم و غیرهوشمند می باشد.

---

[۱] Abbreviation Visual Flight Rules (used under conditions of good visibility)

[۲] Dead Reckoning

[۳] Abbreviation Instrument Flight Rules

[۴] Lower Antenna

[۵] Upper Antenna

[۶] W.R.C.S

(۴) اثرات عمل اختلال، بیشتر از همه بر روی دستگاه های رادار مشاهده میشود، بطوری که غالباً بهره برداری از این دستگاه ها را غیر ممکن می سازد. یکی از راه های مقابله با این نوع عملیات نصب سامانه های مدرن E.C.C.M روی دستگاه‌های رادار میباشد.

ت: تداخل

با استفاده از رمزهای قراردادی بین خدمه پروازی و مرکز کنترل زمینی و تغییر فرکانس رادیویی به راحتی میتوان با این نوع عملیات مقابله نمود.

۱- تکنیک هوشمند

تکنیک پیشرفته و هوشمند ترسیم امواج رادیویی[۱] جنگ الکترونیک توسّط مراکز پژوهشی«دارپا» در امریکا در حال توسعه است و تلاش می‌کند تا امواج هوایی را ترسیم و رصد نموده و ضمن کشف منبع ارسال این امواج، آن را با منابع از پیش تعیین شده خودی تطبیق داده و به خلبان و حتی نیروهای سطحی که از این امواج رادیویی استفاده می‌نمایند این فرصت را بدهد که با چهار پدیده میجی یعنی تداخل، اختلال، اخلال رادیویی و تداخل ناوبری مقابله کند و ضریب اعتماد و قابلیت سامانه‌های ناوبری و رادیویی خود را بهینه و ارتقاء دهند. (رضایی،۱۳۹۳)

میجی در فرآیند عملیات هوایی(کشف و گزارش)

گزارش مستقیم عملیات MIJI هنگام پرواز توسط خدمه پروازی و یا موقع دیگر توسط سایر اپراتورهای ارتباطی در حین فعالیت یا پرواز مجاز نمی باشد. چه در غیر این صورت دشمن از ارزش موثر بودن سامانه های خود آگاه می گردد، لذا فقط به ذکر تهدید و موقعیت تقریبی آن باید اکتفا کرد و سایر مشخصات و اطلاعات مورد نیاز را برابر فرم مربوطه بعد از پایان پرواز یا مأموریت آماده نمود. فرم گزارش مخاطرات میجی یا عملیات فریب ناوبری[۲] حداکثر تا ۲۴ ساعت پس‌از مشاهده باید از طریق یگان مربوطه تکمیل و به مدیریت یا فرماندهی جنگ الکترونیک ارسال گردد.

نحوه گزارش مخاطرات میجی (MHR) در حین فعالیت یا پرواز به منظور آگاهی سایرین از نوع عملیات باید به صورت رمزهای قرار دادی مخابره گردد. نحوه مخابره به این ترتیب است که مشاهده کننده با ذکر کلمه (رمز) و یکی از حروف یاد شده به عنوان مثال A,B,C,D حدود منطقه فعالیت و اطلاعات مورد نیاز را به طور (تقریبی) در اختیار عوامل ذینفع قرار می‌دهد. کلمه (رمز حروف) انتخاب شده می تواند تغییر کند.

- A برای MEACONING
- B برای INTRUSION
- C برای JAMMING
- D برای INTERFERENCE

مثال:

یکی از خدمه پروازی از تداخل ناوبری همراه با تداخل رادیویی اطلاع حاصل نموده و بدین ترتیب (لیدر) دسته پروازی، کنترل رادار، تقرب یا برج مراقبت را آگاه می نماید (مزاحم شماره B,A در ۲۰مایلی شمال مشهد).

برج مراقبت یا کنترلرهای رادار زمینی به محض دریافت چنین خبری مراتب را به پست فرماندهی یا عملیات یگان‌های پروازی موجود در منطقه اعلام نموده و آنها را از وجود فعالیت های فریب ناوبری در منطقه یاد شده آگاه می سازند.

فرماندهی جنگال، مسئولیت اصلی هدایت و رهبری مبارزه و مقابله با پدیده میجی را در فرآیند فریب ناوبری هوایی را به عهده داشته که این مسئولیت را از طریق ارسال بخش نامه ها و دستورالعمل ها به مراکز عملیات پروازی (شکاری و

---

[۱] Radio Wave Mapping

[۲] MIJI Hazard Report

ترابری)، عملیات پدافندی (رادارهای ثابت و متحرک) و فرماندهی های فناوری اطلاعات و ارتباطات و مراکز مخابراتی اعمال و بر حسن اجرای آن نظارت می نماید.

نتیجه گیری

استفاده از امواج الکترومغناطیس برای ارتباطات، مخابرات، تشخیص هدف (رادار)، ناوبری، و شناسایی، بستری مناسب برای عملیات الکترونیکی برای انحراف از بهره برداری در پرواز فراهم می‌سازد. فریب الکترونیک هوانوردی یا اویونیکی یکی از شگرد های رایج جنگ ناوبری هوایی، با هدف حمله به فرایندها و ساختارهای الکترونیکی از قبیل حساسه ها، خطوط ارتباطی، شبکه ها به عنوان ابزارهای مشاهده و تصمیم گیری است، که در سطوح تاکتیکی باعث کاهش کارامدی عملیاتی در پرواز می گردد. زیرا مانع استفاده اثر بخش از طیف امواج الکترومغناطیسی می گردد، که در ادبیات جنگ اطلاعات و زیر مجموعه آن یعنی جنگ الکترونیک به آن میجی[۱](MIJI) گفته می شود. روش های شناسایی و مقابله الکترونیکی و عملیاتی با پدیده میجی به دلیل آسیب پذیری سامانه‌های الکترونیکی هواپیما در برابر این گونه عملیات بسیار مهم و حایز اهمیت است، شناخت این پدیده در حوزه مهندسی هوانوردی این امکان را فراهم می سازد تا برای طراحی سامانه های فریب اویونیکی و پادکنش های(ECM) مرتبط با آن اقدام عملی صورت پذیرد. به همین دلیل کلیه خدمه پروازی، کنترلرهای شکاری، اپراتورهای ارتباطی و مهندسین پرواز باید آموزش های اولیه میجی را طی کلاس های توجیهی کسب و مراتب در پرونده آموزشی آنان منعکس گردد، ضمناً در جلسه های توجیهی روزانه اتفاقات مهم میجی و حل رویداد آن برای کلیه کارکنان ذینفع بازگو و تشریح شود. خدمه پروازی باید قبل از اجرای مأموریت در مناطق خاص و مشکوک، پرونده و سوابق مخاطراتی میجی را که در عملیات پایگاه‌ها نگهداری می شود بررسی ودقت لازم را در اجرای مأموریت بکار برند، ضمناً از پرواز در مناطقی که خطرات میجی آنها تایید گردیده تا حد ممکن اجتناب نمایند. در مأموریت های ناوبری خدمه پروازی باید اصول کار را بر اساس تطبیق عوارض زمین با نقشه قرار داده (ناوبری مستقیم[۲]) و در شرایط نامساعد، از دو سامانه مختلف کمک ناوبری و یا ایستگاه های رادار زمینی استفاده نمایند. کارکنان پروازی وکارکنانی‌که با سامانه‌های پیشرفته الکترونیکی کار می کنند، موظفند که از قوانین و مقررات جاری و دستورالعمل‌های مقابله با فریب‌های ناوبری هوایی تبعیت نموده و هر گونه مورد مشکوکی را از طریق پر کردن فرم (برگ) گزارش مخاطرات MIJI به مراکز عملیات جنگ الکترونیک اعلام نمایند.

---

[۱]-Meaconing, Intrusion, Jamming, Interference(MIJI)

[۲] Dead Reckoning

منابع و ماخذ

ادوارد والتز(۱۹۹۸)، جنگ اطلاعات- اصول و عملیات، مترجمین اکبر رنجبر، حسن حاج قاسم، محمود فخرایی، تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی، چاپ اول ۱۳۸۵

جانسون مارتین و همکاران(۲۰۰۳)، بکارگیری فناوری اطلاعات در طرح ریزی دفاعی در کتاب چالش های نوین ابزارهای نوین برای تصمیم گیری دفاعی، مترجمان محمد جواد زنگنه ، کاظم غریب آبادی ناشر مرکز مطالعات و تحقیقات جنگ سپاه چاپ اول ۱۳۸۴

رضایی،کامران(۱۳۹۳)، مقاله آینده‌پژوهی فناوری‌های راهبردی دارپا، به نقل از سایbusiness Insider در فصلنامه نگاه ۲ ، سال دوّم شماره ۸ زمستان ۱۳۹۳

ستاری خواه ، علی.(۱۳۸۶)، جنگهای الکترونیکی ، تهران، انتشارات وزارت دفاع ، چاپ اول۱۳۸۶

فراتر، میکائیل و میکائیل ری یان(۲۰۰۲)، جنگ الکترونیک، مترجمین احمد عفیفی، مرتضی کریم زاده، محمد باقر نظافتی، تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی، چاپ اول ۱۳۸۵

AFR ٥٥-٣,Departments Of The Air Force, The Army, And The Navy AR ١٠٥-٣,Washington DC ٢٠٣٣٠-٥٠٠٠ OPNAVINST ٣٤٣٠,١٨D, MCO ٣٤٣٠,٣C,٣١ July ١٩٨٦

Arquilla, J., and D. F. Ronfeldt,(١٩٩٣), "Cyber war is Coming!," J. Comparative Strategy, Vol. ١٢, No. ٢, Apr.-June, ١٩٩٣, □□. ١٤١-١٦٥

FM ٢٤-٣٣, Chapter ٤, Meaconing, Intrusion, Jamming, and Interference Reporting

https://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_٠٠٧_alternative_theories#Meaconing

Libicki, M.,(١٩٩٥), "What Is Information Warfare?" Center for Advanced Concepts and Technology, National Defense University, ١٩٩٥, p. ٧.

Lui Sha, lrs(٢٠٠٦), The Complexity Challenge in Modern Avionics Software

Szafranski, R.,(١٩٩٥), "A Theory of Information Warfare: Preparing for ٢٠٢٠," Airpower Journal, Vol. ٩, No. ١, spring ١٩٩٥.

Toffler, Alvin,(١٩٨٠), The Third Wave, New York: Bantam, ١٩٨٠.

Journal of Modern Aviation and Techniques
Year ١, Number ٢, Spring2024

The analysis of the aviation phenomenon of avionic deception (MIJI) and Offering the counter course of Action techniques.

١st NikBakhsh Habibi ٢nd Hassan Shah Safi

Abstract

Due to the vast application of electromagnetic signals in air operations, these signals are always disrupted by enemy in order to obscure the signals that are used in flight. Avionic deception (MIJI) as subdivision of electronic warfare is used as observation and decision making devices with the aim to attack or obstruct electronic structures and processes such as sensors, communication lines and transmitting sources.This type of deception is considered as one of the common techniques of air navigation warfare which limits the effective performance of operation in flight at tactical levels and causing disruption in electromagnetic signals.

In this study it has been attempted to explain the recognition and electronic counter measure methods against MIJI phenomenon and present techniques to nullify it by taking advantages of field and documentation methods along with my flight experience as an aviator.

The obtained results of the study and analysis of this phenomenon show that the pilots and aviators must study and review the records of hazardous MIJI before performing missions in specific and dubious regions.In order to counter with such phenomenon in navigational missions, the pilots must adjust the flight with terrain and charts known as Dead Reckoning (direct navigation) and in unfavorable conditions use the two systems of navigation aid and ground radar stations, and inform the electronic warfare operation center of any suspicious case
through filling out the form of MIJI report.

Keywords: “Avionics”, “Avionic deception”, “MIJI”, “Electronic warfare”, “interference”