فصلنامه علوم و فنون نظامی
سال پانزدهم، شماره ۵۰، زمستان ۱۳۹۸
ص ۱۳۳- ۱۰۷

تاریخ دریافت: ۱۳۹۸/۰۸/۰۴
تاریخ پذیرش: ۱۳۹۸/۱۲/۲۲

بررسی میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر فرآیند تصمیم‌گیری عملیات جنگال در نبرد ناهمتراز

علی پناهی*[1]

چکیده

هدف از انجام این پژوهش، بررسی میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر فرآیند تصمیم‌گیری عملیات جنگال در نبرد ناهمتراز است. ضرورت تحقیق مذکور بر این است که تصمیم‌گیری عملیات جنگال بدون در نظر گرفتن عوامل مؤثر بر فرآیند تصمیم‌گیری و لحاظ نمودن میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر سامانه‌های الکترونیکی دشمن، کیفیت لازم را نخواهد داشت. تحقیق حاضر از حیث روش توصیفی- تحلیلی و ازلحاظ هدف کاربردی است و جامعه موردمطالعه کارکنان گروه ۴۰۲ جنگال نزاجا می‌باشند. یافته‌های پژوهش نشان داد که ارتقاء، بهبود یا اصلاح اقدام جمع‌آوری اخبار الکترونیکی، پردازش و تجزیه‌وتحلیل تهدیدات، بررسی میزان تأثیر تهدیدات الکترونیکی خودی(اختلال، فریب، رمزگشایی، ره‌گیری، شنود و...) بر روی سامانه‌های (ارتباطی) نیروی دشمن، ایجاد یک فرآیند عملیات پشتیبانی الکترونیکی ، کسب اطلاعات الکترونیکی محیط رزم و بررسی میزان تأثیر تهدیدات الکترونیکی غیر ارتباطی نیروهای خودی (اختلال راداری، فریب راداری، شنود راداری، اطلاعات علمی و فنی مسینت‌ها، پنهان نگاری و اختلال ماهواره‌ای، اختلال سایبری) بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا در نبرد ناهمتراز تأثیر زیادی خواهد نمود.

واژه‌های کلیدی:

فرآیند تصمیم‌گیری، عملیات جنگ الکترونیک، تهدید الکترونیکی، نبرد ناهمتراز

---

[1] کارشناس ارشد مدیریت دفاعی

* نویسنده مسئول: Email: alipanahi14@yahoo.com

مقدمه

استفاده از این فناوری جدید بر گستردگی و تنوع سلاح‌ها و جنگ‌افزارها تأثیر شگرفی گذاشت به‌طوری‌که در جنگ‌های امروزی، قدرتی برنده نهایی است که توان استفاده و بهره‌برداری بیشتر از فناوری اطلاعات و تجهیزات الکترونیکی را دارا باشد. ازآنجایی‌که پایه و اساس جنگ‌های نوین و کنونی بر محور اطلاعات، پایه‌ریزی شده‌اند لذا اطلاعات می‌تواند نقش تعیین‌کننده‌ای را در میدان‌ها نبرد جهت کسب نتیجه بهتر و موفقیت سطح کلان ایفا نماید. بر همین اساس هریک از طرفین درگیر که به نحوی بتوانند اطلاعات جامع‌تر و کامل‌تری از قابلیت‌ها و توانایی‌های یکدیگر داشته باشند می‌توانند محکم‌تر و قوی‌تر پا به میدان مبارزه گذاشته و در همان لحظات اول یا روزهای ابتدایی، با کمترین خسارت به پایان برساند (نصیرزاده و شاه‌رضایی، ۱۳۹۱: ۱). پژوهشگران علم مدیریت بر این باورند که تصمیم‌گیری، رکن اساسی تمام وظایف مدیریتی و درعین‌حال، مبنای برنامه‌ریزی است. تصمیم‌گیری در محیط جنگ الکترونیک بسیار خطیر و تعیین‌کننده بوده و فرآیند تصمیم‌گیری در عملیات جنگ الکترونیک به عواملی متعددی همچون: سامانه یا نظام فرماندهی و کنترل جنگ الکترونیک (ستاری‌خواه و مسلمی، ۱۳۹۳: ۴۹)، نیازهای اطلاعاتی و یا ملزومات اطلاعاتی، عوامل محیطی، قابلیت‌های فریب الکترومغناطیسی، ارزیابی عوامل خطرساز جهت تعیین احتمالات خطر (اثربخشی تهدیدات الکترونیکی)، عوامل انسانی جنگ الکترونیک (کارکردهای مدیریتی) و... بستگی دارد (آئین‌نامه جنگ الکترونیک از ام ۳۶-۳: ۷۲-۵۲).

جنگ الکترونیک در نبرد ناهمتراز جهت مقابله با نیروهای فرا منطقه‌ای یکی از عوامل تعیین‌کننده در سرنوشت جنگ است و به‌کارگیری فنون و راه‌کنش‌های متنوع جنگ الکترونیک در نبردهای اخیر، جنگ الکترونیک را عامل بسیار مهم و تعیین‌کننده قدرت برتر صحنه نبرد نموده است بنابراین تصمیم‌گیری در این فضا، الزامات و اقتضائاتی دارد و عواملی بر فرآیند تصمیم‌گیری فرماندهان و مدیران ایفای نقش می‌کنند. در همین راستا بررسی میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر سامانه‌های الکترونیکی نیروهای دشمن، در فرآیند تصمیم‌گیری عملیات جنگ الکترونیک به‌منظور طراحی و اجرای گام‌های بعدی حائز اهمیت است، بنابراین با نگرش به موارد مطروحه، تلاش محقق در این تحقیق بر این است که تأثیر اقدامات الکترونیکی سامانه‌های جنگال گروه ۴۰۲ جنگال را بر سامانه‌های ارتباطی و غیر ارتباطی دشمن احصا و به دنبال آن با برنامه‌ریزی صحیح و متناسب، بر فرآیند تصمیم‌گیری در فضای نبرد ناهمتراز، اثرگذاری نمایند.

مبانی نظری و پیشینه پژوهش

پیشینه پژوهش

با بررسی به‌عمل‌آمده مشخص گردید، در خصوص فرآیند تصمیم‌گیری، مهارت‌های مدیریتی و عملیات جنگ الکترونیک، چند تحقیق صورت گرفته که خلاصه‌ای از آن‌ها به شرح زیر است:

جدول (۱) پیشینه تحقیق

پژوهشگر	عنوان پژوهش	نتایج پژوهش
آقای علی‌رضا خالقی (مهرماه ۱۳۹۲، دافوس آجا)	نحوه ارتقاء توانمندی جنگال	سؤال اصلی: نحوه ارتقاء توانمندی جنگال (دانش، تجهیزات، آمایش) چگونه باید باشد؟ نتایج تحقیق: الف: برای ارتقاء دانش باید به تهدیدات خارجی و آسیب‌های داخلی توجه گردیده و متناسب با آن نسبت به ارتقاء دانش تخصصی اقدام گردد. ب: برای ارتقاء دانش تخصصی برگزاری رزمایش‌ها و شرکت گسترده کارکنان در آن امری الزامی است. ج: خطرپذیری جمع‌آوری سیگنالی توسط جنگال بسیار پایین‌تر از جمع‌آوری انسانی است. د: صحت جمع‌آوری اخبار و اطلاعات توسط جنگال بیشتر از سایر طرق جمع‌آوری مورد تأیید است.
آقای علی‌رضا قاسمی، (تیرماه ۱۳۸۸، دافوس آجا)	یگان‌های مناسب عملیات جنگال نزاجا در مقابله با تهدیدات جنگ الکترونیک نیروهای فرا منطقه‌ای.	سؤال اصلی: یگان‌های مناسب عملیات جنگال نزاجا (تجهیزات، نیروی انسانی و تحرک مناسب) در مقابله با تهدیدات جنگ الکترونیک نیروهای فرا منطقه‌ای چگونه باید باشد؟ نتایج تحقیق: الف: آموزش نیروی انسانی بایستی در راستای فناوری روز و متناسب با تهدیدات فرا منطقه‌ای بوده و مبتنی بر عمل و تهدید و بر پایه تخصصی باشد. ب: کارکنان بایستی توانایی کار با سیستم‌های نوین و توانایی جمع‌آوری، پردازش و گزارش هرگونه اخبار را داشته و بتوانند آموزش‌های مختلف را فراگیرند. ج: کارکنان بایستی مسلط به زبان‌های خارجی مانند انگلیسی، عربی، اردو، پشتو، ترکی، آذری، عبری، آلمانی، فرانسوی و سایر زبان‌ها بوده و از تحصیلات علمی بالا جهت بهره‌گیری از فنّاوری جدید و به‌کارگیری مناسب و مطلوب تجهیزات متناسب با فناوری روز برخوردار باشد.
آقای محمدتقی باقری	بررسی رابطه دانش	مسئله: آیا بین دانش مدیریتی (برنامه‌ریزی، تصمیم‌گیری،

دانشجوی دوره پانزدهم دافوس آجا	مدیریتی مدیران نزاجا (مستقر در تهران) و عملکرد آن‌ها	سازمان‌دهی، ارتباط، نظارت و کنترل و رهبری) مدیران میانی نزاجا (مستقر در تهران) و عملکرد آن‌ها رابطه معنی‌داری وجود دارد؟ نتیجه تحقیق:یافته‌های تحقیق نشان می‌دهد بین دانش مدیریتی (برنامه‌ریزی، تصمیم‌گیری، سازمان‌دهی، ارتباط، نظارت و کنترل و رهبری) مدیران میانی نزاجا و عملکرد آن‌ها رابطه معنی‌داری (با شدت بالا) وجود دارد.

مبانی نظری

فرآیند تصمیم‌گیری

تصمیم‌گیری فرآیندی است که با آن راه‌حل مسئله را به‌طور معین انتخاب می‌کنیم فرآیند انتخاب مشتمل بر مجموعه فعالیت‌هایی است که به گزینش یک راه‌کار از مجموعه راه‌کارها می‌انجامد بنابراین فرآیند انتخاب، جزئی از فرآیند تصمیم‌گیری است.(گودرزی، محمدعلی و همکاران، ۱۳۹۸ : ۷۸)

به‌طورکلی فرآیند تصمیم‌گیری را می‌توانیم شامل ۷ مرحله بدانیم.

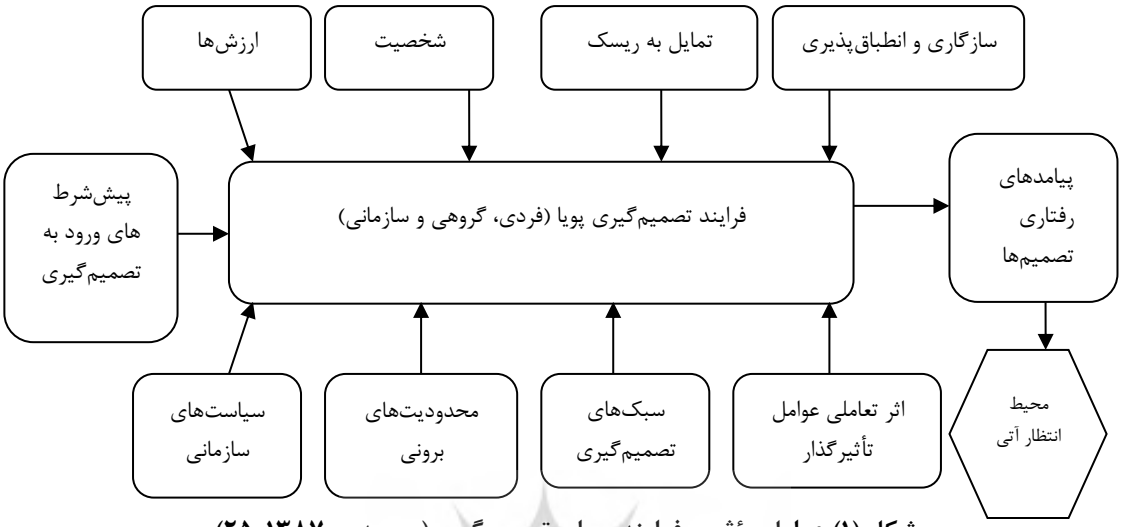
جدول (۲) فرآیند تصمیم‌گیری نظامی(FM5-0c1,2012)

ورودی‌های کلیدی	مراحل	خروجی‌های کلیدی
طرح یا دستور رده‌بالا پیش‌بینی مأموریت جدید	مرحله اول دریافت مأموریت	راهنمای مقدماتی فرماندهان اختصاص اولیه زمان
طرح یا دستور رده‌بالا دانش و اطلاعات پرورش‌یافته رده‌بالا دانش سایر سازمان‌ها طراحی مفهوم فرضیات	مرحله دوم تجزیه‌وتحلیل مأموریت	بیان مسئله بیان مأموریت مقصود اولیه فرماندهان راهنمای طرح‌ریزی اولیه عناصر اصلی اطلاعات خودی
بیان مأموریت مقصود اولیه فرماندهان به‌روز کردن آمادگی اطلاعاتی منطقه نبرد فرضیات	مرحله سوم توسعه راه‌کارها	بیان راه‌کارها و طرح‌ها سازمان‌دهی از مایشی وظایف مفاهیم عملیات تجدیدنظر راهنمای طرح‌ریزی فرضیات به‌روز شده

برآوردهای جاری به‌روز شده تجدیدنظر در راهنمای طرح‌ریزی بیان راهکارها و طرح‌ها فرضیات به‌روز شده	مرحله چهارم تجزیه‌وتحلیل راه‌کارها (بازی جنگ)	راه‌کارهای اصلاح‌شده نکات بالقوه تصمیم نتایج بازی جنگ ارزیابی مقدماتی فرضیات به‌روز شده
برآوردهای جاری به‌روز شده اصلاحات راه‌کارها ارزیابی شاخص‌ها نتایج بازی جنگ فرضیات به‌روز شده	مرحله پنجم مقایسه راه‌کارها	راه‌کارهای ارزیابی‌شده راهکارهای پیشنهادی برآوردهای جاری به‌روز شده فرضیات به‌روز شده
راهکارهای پیشنهادی راه‌کارهای ارزیابی‌شده برآوردهای جاری به‌روز شده فرضیات به‌روز شده	مرحله ششم تصویب راه‌کارها	راه‌کار انتخاب‌شده بدون هیچ اصلاح اصلاح مقصود فرماندهان نیازمندی اطلاعات فرماندهان عناصر اصلی اطلاعات خودی
راه‌کار انتخاب‌شده بدون هیچ اصلاح اصلاح مقصود فرماندهان نیازمندی اطلاعات فرماندهان عناصر اصلی اطلاعات خودی	مرحله هفتم دستورها	تصویب طرح عملیاتی یا دستور

عوامل مؤثر بر فرآیند تصمیم‌گیری

فرایند تصمیم‌گیری سه رکن اساسی دارد که به وجود مسئله ماهیت می‌دهند سه جزء مسئله یا موقعیت ، تصمیم‌گیرنده و محیطی که در آن مسئله رخداده است اجزای اصلی مسئله را شکل می‌دهند تصمیم‌گیری درست، نیازمند شناخت و توجه به هر سه عامل اساسی در تصمیم‌گیری است (گودرزی و همکاران،۱۳۹۷). تصمیم‌گیری از وظایف اصلی مدیران به شمار می‌آید و تحقق اهداف سازمان به کیفیت آن بستگی دارد. این امر مهم تحت تأثیر تعداد زیادی عوامل قرار دارد که با توجه به ماهیت سازمان تصمیم‌گیرنده، موقعیت تصمیم گیر، سطح تصمیم‌گیری و ... وزن این عوامل نیز متفاوت است. در سازمان‌های نظامی دو عامل اطلاعات و زمان از مهم‌ترین عوامل تأثیرگذار بر کیفیت تصمیم‌گیری به شمار می‌آیند. برای تصمیم‌گیری ، قبل از هر چیز به اطلاعات نیاز است ، در تصمیم‌گیری، نه‌تنها کیفیت اطلاعات، بلکه مقدار اطلاعاتی که گردآوری و تحلیل می‌شود نیز اهمیت دارد (ولی وند زمانی، حسین، ۱۳۹۸: ۱۶).



شکل (۱) عوامل مؤثر بر فرایند پویای تصمیم‌گیری(حمیدی، ۱۳۸۷: ۲۵)

جنگ الکترونیک [1]

جنگ الکترونیک عبارت است از یک عمل نظامی که شامل به‌کارگیری انرژی الکترومغناطیسی و انرژی مستقیم برای کنترل طیف الکترومغناطیس و یا حمله به دشمن(آیین‌نامه جی پی۳-۱۳-۱)، توانمندی و ظرفیت جنگ الکترونیک، به‌گونه‌ای است که نیروهای نظامی را برای ایجاد شرایط و اثرگذاری در طیف الکترومغناطیس برای پشتیبانی از نیات و تدابیر عملیاتی فرماندهان قادر می‌سازد. جنگ الکترونیک شامل حمله الکترونیکی[2]، حفاظت الکترونیک[3] و پشتیبانی الکترونیکی[4]است و شامل فعالیت‌هایی مانند پارازیت رسانی، ره‌گیری، کشف و شناسایی، وانمود سازی، پشتیبانی، توانمندسازی، محافظت و گردآوری ظرفیت‌های عملیاتی از طریق طیف الکترومغناطیس و بهره‌برداری از ظرفیت‌های فضای سایبری است(FM3-12,2017)

---

[1]- Electronic warfare
[2]- EA: Electronic Attack
[3] -EP: Electronic Protection
[4] -ES: Electronic Support

جنگ الکترونیک در رابطه با سیگینت یا اطلاعات سیگنالی دارای دو مؤلفه اصلی است: اطلاعات مخابراتی یا کامینت[1] و اطلاعات الکترونیکی یا الینت[2] به‌طورکلی این دسته از اطلاعات حوزه عملکرد جنگ الکترونیک ارتباطی و غیر ارتباطی را منعکس می‌کنند اما در محیطی راهبردی به‌جای محیط تاکتیکی رخ می‌دهند (نباتی، ۱۳۹۱: ۵۰).

مفهوم عملیات جنگ الکترونیک

عملیات جنگ الکترونیک عبارت است از پیاده‌سازی، کنترل، بهره‌گیری و نفوذ در طیف الکترومغناطیس دشمن به‌گونه‌ای که اطلاعات موردنیاز سامانه‌ی فرماندهی را تأمین نماید؛ و در صورت اراده فرماندهی، دشمن را از بهره‌برداری از طیف الکترومغناطیس محروم و امکان حداکثر بهره‌برداری از طیف الکترومغناطیس را برای نیروهای خودی فراهم سازد.

اجرای عملیات صحیح مستلزم رعایت اصولی است تا بتواند عملیات جنگ الکترونیک در عملیات رزمی تأثیرگذار شود. اولین گام، تقسیم اقدامات هم‌سنخ و گام بعدی تعیین سطوح این اقدامات است. سپس، چگونگی ارتباط این اقدامات با یکدیگر از سویی و ارتباط آن با سایر ارکان فرماندهی مشخص می‌شود (واحدی، ۱۳۹۰: ۱۴۱).

فرآیند عملیات جنگ الکترونیک

فرآیند عملیات، حول محور فرماندهی آگاه از روش فرماندهی عملیات (مأموریت)، در مورد فعالیت‌های برنامه‌ریزی، آماده‌سازی، اجرا و ارزیابی عملیات نظامی، در گردش است. این اقدامات ممکن است به‌طور متوالی و یا بی‌وقفه در سرتاسر یک عملیات انجام‌پذیرند و در صورت لزوم تکرار شده و با یکدیگر تداخل داشته باشند (شکل ۲). افسر جنگ الکترونیک به‌طور فعال در فرآیند عملیات درگیر است. برنامه‌ریزی، آماده‌سازی، اجرا و ارزیابی جنگ الکترونیک مستلزم دانش، مهارت و تخصص جمعی عوامل در مورد عملیات‌ها، جاسوسی، سیگنال و فرماندهی مأموریت است، افسر جنگ الکترونیک تلاش‌های به‌عمل‌آمده در سرتاسر مأموریت-های جنگی را، جهت اطمینان از پشتیبانی عملیات جنگ الکترونیک و حمایت از اهداف فرمانده، هماهنگ می‌سازد (از ام ۳۶-۳ آئین‌نامه جنگ الکترونیک: ۵۰).

---

[1]- Comint = Communication Intelligence
[2]- Elint = Electronic Intelligence

شکل (۲) فرآیند عملیات‌ها (FM3-36,2012)

فرآیند تصمیم‌گیری جنگ الکترونیک

طرح‌ریزی جنگ الکترونیک بر سه اصل استوار است. اولین اصل، به‌کارگیری فرآیند تصمیم-گیری نظامی است[1]. طراحان جنگ الکترونیک هفت مرحله را برای فرآیند تصمیم‌گیری نظامی در نظر گرفته و از آن پیروی می‌کنند و در شرایطی که با مشکل کمبود زمان مواجه باشند همچنان هر هفت مرحله را دنبال کرده و به خلاصه کردن مناسب این فرآیند اقدام می‌کنند. طرح‌ریزی جنگ الکترونیک بر سه اصل استوار است. اولین اصل به‌کارگیری فرآیند تصمیم-گیری نظامی است که به شرح زیر به آن اشاره می‌گردد:

مرحله اول: دریافت مأموریت

مرحله دوم:تجزیه‌وتحلیل مأموریت

مرحله سوم: روند توسعه عملیات

مرحله چهارم: تجزیه‌وتحلیل روند عملیات (رزمایش)

مرحله پنجم: مقایسه روند عملیات

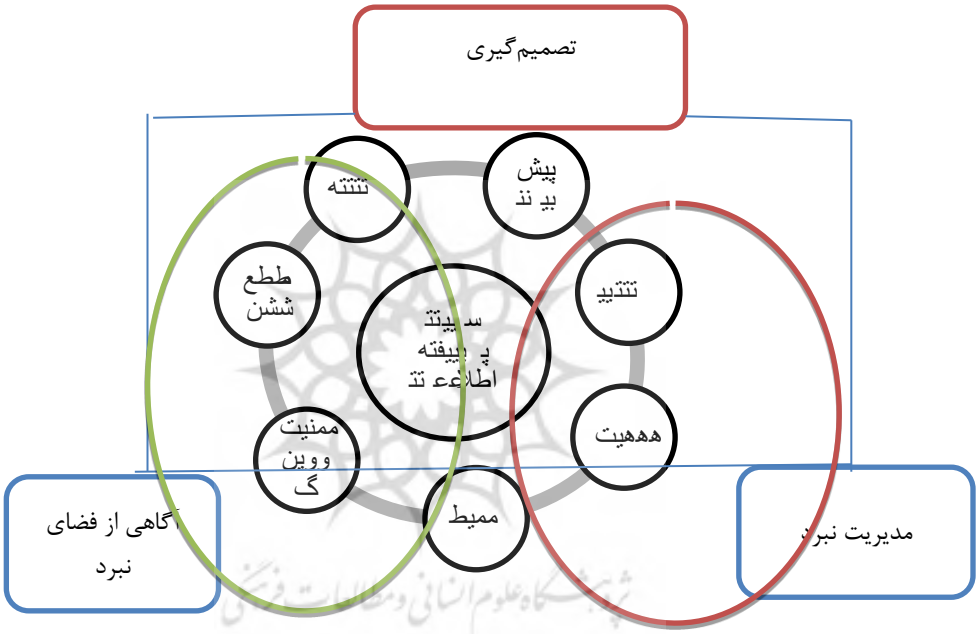
مرحله ششم: تأیید و تصویب روند عملیات

مرحله هفتم: تهیه و ارائه دستورات(آیین‌نامه عملیات مشترک جنگ الکترونیک ۱۳۹۷: ۱۹۵)

[1] . military decision making process

برنامه‌ریزی جنگ الکترونیک همگام و هم‌زمان با سایر برنامه‌ریزی‌های عملیاتی در طی فرآیند تصمیم‌گیری نظامی اتفاق می‌افتد. در حین فرآیند تصمیم‌گیری نظامی چندین فرآیند از قبیل فراهم‌سازی کسب اطلاع از صحنه نبرد (تأمین جاسوسی صحنه نبرد)، فرآیند هدف‌گیری و مدیریت احتمال خطر و ضرر و زیان، همگام و هم‌زمان به اجرا درمی‌آیند.(اف- ام ۳۶-۳ : ۵۳)

یکی از اهداف جنگ الکترونیک آگاهی از فضای نبرد و ایجاد فرآیندی مناسب و کارا در تصمیم‌گیری در میدان نبرد است. شکل ۳ تصویر فرآیند یادشده را نشان می‌دهد.



شکل (۳) فرآیند تصمیم‌گیری با بهره‌گیری از بانک اطلاعات (واحدی، ۱۳۹۰: ۱۷۱)

جنگ ناهمتراز

جنگی محدود، میان دو نیروی نظامی است که توان رزمی محسوس یکی از طرفین نسبت به دیگری، در زمان و مکان عملیات، برتری قابل‌توجه داشته باشد و در آن جنگ نیروی با توان رزمی کمتر باانگیزه معنوی، مقابله همه‌جانبه‌ی اثربخش را اجرا می‌نماید. نیروی برتر در عملیات ناهمتراز به دلیل داشتن توان رزمی بیش از شش برابر، پیروزی را با احتمال ۹۵ درصد انتظار دارد؛ بنابراین تاکتیک اتخاذشده برای مقابله با نیروی ناهمتراز، ابتدا بایستی برتری توان رزمی و سایر برتری‌های دشمن را خنثی نماید. (شیخ، محمدرضا و همکاران ۱۳۹۷: ۴۲-۴۱)

موفقیت جنگ الکترونیک در رزم ناهمتراز

موفقیت در نبردهای امروزی به سه مؤلفه‌ی اصلی زیر بستگی دارد:

۱) سامانه‌ها و جنگ‌افزاری‌های مجهز به حساسه‌های پیشرفته‌ی جنگالی؛
۲) نیروی انسانی متخصص، مجرب و کارآمد به‌عنوان سرمایه انسانی واجد شرایط؛
۳) سامانه یا نظام فرماندهی و کنترل پویا، منعطف، شبکه‌مدار و متناسب با تهدیدهای منطقه‌ای و فرا منطقه‌ای(ستاری خواه، علی و مسلمی، حسین،-۱۳۹۳ :۶۲)

کارکرد اجزایی جنگ الکترونیک در جنگ ناهمتراز

در جنگ ناهمتراز با توجه به قدرت دشمن و هم‌پیمانانشان ازنظر برتری در فنّاوری، تنوع تجهیزات، آموزش و... باید قبل از شروع نبرد بیشترین فعالیت جنگال به جمع‌آوری اطلاعات سیگنالی متکی باشد و در حین اجرای عملیات حداکثر توجه به سیستم‌های ارتباطی و الکترونیکی خودی ازنظر حفاظت الکترونیکی به‌منظور حفظ انسجام نیروهای خودی معطوف شود و همچنین نباید نسبت به منحرف نمودن موشک‌ها و هواپیماهای دشمن با استفاده از فن‌ها و تاکتیک‌های آفند الکترونیکی غافل شد. همچنین باید با استفاده از اطلاعات به‌دست‌آمده توسط یگان‌های اطلاعات سیگنالی و پشتیبانی الکترونیکی، نسبت به پیدا کردن نقاط ضعف ارتباطی و الکترونیکی دشمن و وارد آوردن ضربات ناگهانی به آن نقاط، باعث تزلزل روحیه دشمن و درنتیجه کاهش توان رزمی او شد(فلاحی, احمدرضا – ۱۳۹۰ :۴۷)

مؤلفه‌های تعیین سطوح اقدام جنگ الکترونیک

مؤلفه‌های گوناگونی در تعیین سطوح اقدام جنگ الکترونیک تأثیر دارد. ازجمله مؤلفه‌های اصلی می‌توان از مؤلفه‌های نوع هدف و تهدید، عمق هدف و تهدید، مدت‌زمان فعالیت و کنترل، مقطع زمانی فعالیت، باند فرکانسی، میزان تجزیه‌وتحلیل فنی، توان پیاده‌سازی و روش مدیریتی نام برد. برای مقایسه سطوح اقدامات راهبردی، عملیاتی و تاکتیکی و درک صحیح آن جدول ۱ ترسیم‌شده است.

جدول (۳) مقایسه سطوح اقدام جنگ الکترونیک(واحدی مرتضی ،۱۳۹۰: ۱۴۶)

شاخص‌ها	راهبردی	عملیاتی	تاکتیکی
نوع هدف	سیاسی، اقتصادی نظامی، وزارت دفاع، ستاد نیروهای مسلح و کلیه قرارگاه‌های نظامی خاص	نظامی تا قرارگاه سپاه	نظامی تا رده قرارگاه لشگر
عمق هدف	حداقل ۲۰۰ کیلومتر	۱۰۰ کیلومتر	۴۰ کیلومتر
مدت‌زمان فعالیت	مستمر – شبانه‌روزی	شبانه‌روزی	بنا به دستور
مقطع زمانی فعالیت	صلح – بحران - جنگ	بحران – جنگ	بنا به دستور
باند فرکانسی	کل طیف الکترومغناطیس	کل طیف الکترومغناطیس	کل طیف الکترومغناطیس
میزان تجزیه‌وتحلیل فنی (توان پیاده‌سازی)	رمزشکنی پیاده‌سازی الگوریتم‌ها و پروتکل تا دسترسی به متن آنالیز سیگنال‌های ناشناخته	بهره‌برداری از سامانه‌های آماده برای پیاده‌سازی سیگنال نمونه‌برداری از سیگنال‌های ناشناخته	بهره‌برداری از سامانه‌های آماده برای پیاده‌سازی سیگنال تجزیه تحلیل در حد کشف سیگنال و پیاده‌سازی ارتباطات تاکتیکی
روش مدیریتی	مدیریت متمرکز و یکپارچه	بنا به مأموریت	بنا به مأموریت

عوامل مؤثر بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک

الف- سامانه یا نظام فرماندهی و کنترل جنگ الکترونیک

ب-نیازهای اطلاعاتی و یا ملزومات اطلاعاتی

پ-عوامل محیطی

ت- قابلیت‌های فریب الکترومغناطیسی

ث- ارزیابی عوامل خطرساز جهت تعیین احتمالات خطر(اثربخشی تهدیدات الکترونیکی)

ج-عوامل انسانی جنگ الکترونیک(کارکردهای مدیریتی)

چ-سایر عوامل.(نصیر زاده، عزیز- شاه رضایی محمدحسن- ۱۳۹۱ : ۱)

تهدید الکترونیکی

تهدید الکترونیکی در نگاه کلی عبارت است از عامل بازدارنده‌ی خارجی، غیرطبیعی (مصنوعی) و عمدی که به‌صورت الکترونیکی یا غیر الکترونیکیِ عامل (فعال) یا غیرعامل (غیرفعال) موجب اختلال و بهره‌برداری افراد، سازمان‌ها و کشورهای متخاصم یا غیرمجاز از سامانه‌ها و شبکه‌های ارتباطی، الکترونیکی، الکترواپتیکی و...خودی با استفاده از روش‌ها و سامانه‌های غیرمجاز، جهت ممانعت از دست‌یابی نیروهای خودی به مقاصد امنیت الکترونیکی و ارتباطی گفته می‌شود این تهدیدها دارای مظاهری است که مهم‌ترین آن‌ها در عرصه ملی عبارت است:

۱- از کار انداختن یا اختلال در سامانه‌های اطلاعاتی شبکه‌ای که به‌صورت حمله‌های تغییردهنده سامانه و حمله‌هایی که تمامیت اطلاعات را تهدید می‌کنند، انجام می‌شود.

۲- حمله به زیرساخت‌های حساس عمومی نظیر از بین بردن زیرساخت‌های اطلاعات و ارتباطات و جاسوسی یا سرقت اطلاعات.

۳- وابستگی شدید در بهره‌برداری از شبکه‌ها و فضای مجازی نظیر وابستگی زیرساخت‌ها، وابستگی در اجزای فناوری (نرم‌افزار، سخت‌افزار، شبکه و...)

٤- کاهش کنترل‌های رسمی به علت وجود و توسعه شبکه‌های جهانی و وابستگی به آن‌ها .

قابلیت‌ها (توانایی‌ها) یک عامل مخاطره انگیز است و این قابلیت‌ها می‌تواند جنبه علمی و فنی داشته باشد. در عرصه فناوری اطلاعات و ارتباطات بنا به ماهیت انتشار امواج و عرصه‌های

مختلف این توسعه تهدیدهای الکترونیکی از دو جنبه عامل و غیرعامل برخوردار است که جنبه عامل بودن تهدید به برخورداری از انتشار امواج یا هر عامل عمل‌کننده نظیر بمباران و ... است و جنبه غیرعامل بودن آن دربرگیرنده اقداماتی است که فاقد اثرات انتشاری، انهدامی یا تخریبی و غیره را در برمی‌گیرد.

نمودار (۱) تنوع تهدیدهای الکترونیکی از جنبه‌های عامل/غیرعامل(مسلمی حسین -۱۳۹۱)

پیروزی و شکست در جنگ مرهون برنامه‌ریزی و آمادگی نیروها در مواجه با تهدید است. تهدید شناسی و مقابله با تهدیدات الکترونیکی در جنگ‌های اخیر نیروهای فرا منطقه‌ای در خاورمیانه تنها از روش‌های علّی و معلولی امکان‌پذیر نیست، بلکه برای تهدیدشناسی و کسب آمادگی لازم جهت مقابله با آن باید در ابتدا تدابیر لازم مبتنی بر مطالعه روندهای اخیر و آینده‌پژوهی تهدیدات و محیط جنگ آینده اخذ و آموزش‌ها و سازمان‌دهی مناسب داده شود. (مسلمی حسین ۱۳۹۱ :۴۵). (شایان‌ذکر است در این تحقیق، بررسی تهدیدات الکترونیکی، بر مبنای تهدیدات زمین پایه ارتش آمریکا لحاظ شده است).

اثربخشی تهدیدات الکترونیکی ارتباطی

در رویکرد تأثیرمحور باید بیش از کارایی به اثربخشی توجه شود.کارایی به‌عنوان مقوله‌ای کمی عمدتاً قابلیت‌های فنی و سخت‌افزاری را شامل می‌شود. اما این نگاه لزوماً با فلسفه تأثیرمحور هم‌خوانی ندارد. فلسفه تأثیرمحور بر اثربخشی اقدامات تأکید دارد که امری است کاملاً کیفی، بدیهی است که معیارهای سنجش کارایی و اثربخشی با یکدیگر متفاوت می‌باشند. در بازیگران فناوری، آگاهی وضعیتی چیزی بیش از سازمان رزمی و آرایش یگان‌های دشمن را شامل شده و مواردی مانند پایش تغییرات در رفتار بازیگران مختلف، پیش‌بینی اقدامات آن‌ها و یافتن نقاط حیاتی و آسیب‌پذیر در سیستم دشمن را نیز در برمی‌گیرد که سخت نیازمند سامانه‌های پیشرفته جمع‌آوری و تحلیل اطلاعات است . (مختار زاده و مسلمی ۱۳۹۱)

تهدیدات ارتباطی

تهدیدات ارتباطی شامل شبکه‌های ارتباطی زمین پایه ، دریا پایه ، هواپایه و فضاپایه از اهداف عملیات جنگ الکترونیک می‌باشند .

الف- شبکه ارتباط‌های تاکتیکی :

(۱) ارتباط اچ -از

(۲) ارتباط وی/ یو اچ از

(۳) ارتباط وی ال از

(۴) ارتباط سطح به هوا ، هوا به هوا و سطح به سطح : مانند لینک ۱۶ و لینک ۲۲

ب- ارتباط‌های نقطه‌به‌نقطه رادیویی

رادیو دیتای باندهای یو اچ از /اس اچ از/ ای اچ از۱

رادیو تروپو

(۱) ارتباط ماهواره‌ای باندهای یو اچ از /اس اچ از/ ای اچ از

1. HUF/SHF/EHF

پ- ارتباط سلولار

(۱) تجاری : جی اس ام ، سی دی ام آ، وایمکس، وایفای، ال تی ای [1]

(۲) ارتباط ماهواره‌ای سیار : ثریا ، اریدیوم ، اینمارست و ...

(۳) شبکه‌های سلولار سیار نظامی

ت- رادیو لینک پهپادها

ث- رادیو کنترل پهپادها

حمله الکترونیکی

این تقسیم‌بندی بر اساس نوع نتیجه اقدام آفندی است که خود به انهدام سخت و انهدام نرم تقسیم می‌شود و دیگری بر اساس ماهیت اقدام است که به آفند الکترونیکی فعال و غیرفعال تقسیم می‌شود که در زیر شرح داده می‌شود.

الف- انهدام سخت

انهدام سخت، اقدام آفندی است نتیجه آن خرابی سامانه‌های مورد هجوم یا به‌عبارتی‌دیگر، سوختن برخی مدارات به‌ویژه مدارات ورودی و خروجی همچون بخش آنتن و تغذیه آن‌ها است. بهره‌برداری از سامانه مورد هجوم حتی پس از توقف آفند نیز امکان‌پذیر نخواهد بود. زمانی که قطع ارتباطات فرماندهی و کنترل دشمن مهم‌تر از استفاده از آن برای جمع‌آوری اطلاعات یا فریب الکترونیکی باشد این نوع آفند بهترین راه برای فرماندهان است(واحدی، مرتضی و قیاسی، علی‌اکبر، ۱۳۹۰ :۸۶)

ب- انهدام نرم (اخلال)

انهدام نرم یا اخلال اقدام آفندی است که نتیجه آن جلوگیری یا کاهش گیرندگی سامانه‌های ارتباطی و الکترونیکی مورد هجوم است. در این نوع اقدام بهره‌برداری مجدد از سامانه هجوم پس از توقف آفند امکان‌پذیر است. موارد زیر ازجمله اقدامات آفندی انهدام نرم محسوب می‌گردد.

---

1. GSM ،CDMA ، WiMAX ،WiFi ، LTE

اخلال (جمینگ) سامانه‌های راداری

اخلال (جمینگ) سامانه‌های مخابراتی

اخلال (جمینگ) سامانه‌های تسلیحاتی

ایجاد اهداف مجازی (چف و فیلر)

فریبنده‌های راداری (دکوی)

اختلال ارتباطی

فعالیت جنگال در تمام طیف عملیات نظامی قابل به‌کارگیری هستند و به زمان جنگ محدود نمی‌شوند در زمان صلح، ارتش‌ها سعی می‌کنند منبع انتشار الکترونیکی دشمن را شنود، تعیین موقعیت و شناسایی کنند. سپس توسط آنالیز و تجزیه‌وتحلیل جزئیات مناسبی از قابلیت‌ها و آسیب‌پذیری‌هایی که در زمان جنگ مثمر ثمر خواهند بود اطلاعات لازم را استخراج خواهد شد این فرآیند که به اطلاعات سیگنالی و یا سیگنت معروف است نقش تعیین‌کننده‌ای در تضمین موفقیت جنگ الکترونیک بر عهده دارد سیگنت به‌عنوان تغذیه‌کننده جنگ الکترونیک اطلاعات ذی‌قیمت ی از سامانه‌های ارتباطی، راداری، ناوبری و موشکی در اختیار واحدهای جنگال قرار می‌دهد. هدف از جمینگ مخابراتی جلوگیری از انتقال اطلاعات است. جمینگ مخابراتی به مدولاسیون سیگنال، هندسه لینک و توان سیگنال ارسال‌شده بستگی دارد (جعفری، سید بهزاد و همکاران-۱۳۹۲ :۳۴۴). هدف از اختلال در ارتباطات، مختل نمودن سامانه‌های ارتباطی دشمن از طریق ارسال توانی بیشتر از توان فرستنده‌های شبکه و سپس به گیرنده‌های شبکه است. فقط گیرنده‌ها دچار اختلال می‌شوند. حمله الکترونیکی می‌تواند سامانه‌های مخابراتی دشمن را از طریق اختلال، فریب و خنثی‌سازی، تجهیزات ره‌گی ر شنود را به همین روش و تجهیزات الکترونیکی را از طریق خنثی‌سازی مورد هدف قرار دهد، اهداف اخلال ارتباطی شامل موارد زیر است:

۱- اخلال ارتباطی شبکه‌های فرماندهی و کنترل به‌منظور کاهش توان رزمی دشمن

۲- اخلال ارتباطی شبکه ارتباطی کنترل آتش پدافند هوایی برای جلوگیری از کاربرد مؤثر آن.

۳- وادار کردن دشمن به برقراری سامانه‌های ارتباط پشتیبان که سبب اتلاف نیروی انسانی، تجهیزات و زمان می‌شود.

۴- اخلال ارتباطی سامانه‌های ارتباطی دشمن جهت محدود کردن و کاهش برد مفید آن‌ها
۵- فریب کاربران ارتباطی و وادار کردن آن‌ها به شکستن امنیت ارتباطات و رمز
۶- اخلال در محیط به صورت‌های اخلال طبیعی که درنتیجه فعالیت جو و زمین (مانند رعدوبرق، طوفان‌های خورشیدی و ...) ناشی می‌شود.
۷-اخلال مصنوعی که ناشی از مصنوعات بشری (مانند کابل‌های فشارقوی، فرستنده‌های قوی، موتوربرق‌ها و...) است به وجود می‌آید. ممکن است اخلال به‌صورت عمدی انجام شود که در این صورت یک اقدام آفند الکترونیکی محسوب می‌گردد و امکان دارد به‌صورت غیرعمدی رخ دهد که ناشی از طبیعت یا مصنوعات بشری باشد. (واحدی، و قیاسی، ۱۳۹۰ :۹۲)

اثربخشی فریب الکترونیکی

هدف از فریب الکترونیکی گمراه نمودن وی و گ یج کردن دشمن است و همانند سایر شکل‌های آفندی جنگال،فریب الکترونیکی نیز به‌صورت جداگانه عملی نیست، درواقع قسمتی از طرح فریب تاکتیکی بوده و به‌نوبه خود بخشی از نقشه سرا سری فرماندهی است. انواع اصلی فریب‌های الکترونیکی بدین گونه می‌باشند:۱- تغییر اثرات تجهیزات خودی با عوض کردن خصوصیات الکترونیک تجهیزات تشعشعات مخابراتی و غی ر مخابراتی که به فریب جعلی[1] معروف است. ۲- استفاده از ترافیک و مخابرات دروغین و سامانه‌های الکترونیکی برای ساختن نمایی از یک نیرو، در یک موقعیت مکانی اشتباهی و با توانایی متفاوت، که به فریب الکترونیکی شبیه‌سازی[2] معروف است.۳- نفوذ به سامانه‌های مخابراتی دشمن جهت گمراه نمودن آن‌ها و به دست آوردن اطلاعات که فریب الکترونیکی تقلیدی[3] نام دارد.

[1]Manipulative
2.Simulative
[3]Imitative

اثرپذیری صوت در مقابل اختلال

برای صوت، از دست دادن داده به خاطر اختلالات باعث به وجود آمدن خش‌خش‌هایی می‌شود که می‌تواند آزاردهنده باشد. اگرچه قابلیت فهم صوت به‌صورت آرام افت می‌کند. زیرا حتی اگر به‌صورت دیجیتالی کد و فشرده‌سازی شود، سامانه شنوایی انسان خطاهای حاصل از این تبدیل را احساس نمی‌کند. درصورتی‌که تقریباً یک‌سوم و یا بیشتر از کل داده صوت به خاطر تداخل با دیگر سیگنال‌های معمولی و یا پرش دار خراب شوند قابلیت فهم صوت از بین خواهد رفت.

اخلال ارتباط ماهواره‌ای

بخش مهمی از مأموریت آفند ارتباطی، آفند الکترونیکی روی ارتباطات ماهواره‌ای است. شبکه ارتباطی ماهواره‌ای دشمن، هدفی مهم برای شنود یا مختل کردن است. ماهواره‌های ارتباطی، اطلاعات دیجیتال را از بین نقاط مختلف روی زمین یا نزدیک به سطح زمین تبادل می‌کنند (واحدی، مرتضی و قیاسی، علی‌اکبر ۱۳۹۰ : ۱۰۱)

خنثی‌سازی

مفهومی است که در آن از یک انرژی الکترومغناطیسی سطح بالا، برای قطع کردن و یا از کار انداختن دائمی عملیات تجهیزات الکترونیکی دشمن استفاده می‌شود. این توان موردنیاز از مقدار توان لازم برای فریب و ارتباطات نیز بیشتر است. نه‌تنها سامانه‌های مخابراتی، بلکه تمامی تجهیزات الکترونیکی و حتی بعضی از سامانه‌های غیر الکترونیکی نیز پتانسیل آسیب‌پذیری در برابر سلاح‌های خنثی‌سازی را دارند. درگذشته خنثی‌سازی تنها بر روی علائم الکترومغناطیس متمرکزشده بود درحالی‌که اخیراً امکان ساخت سلاح‌های خنثی‌سازی غیرهسته‌ای بر پایه فناوری توان بالاتر آر- از فراهم‌شده است. این سلاح‌ها توانایی زیان رساندن، کور کردن، منقطع کردن و یا حتی خراب کردن تجهیزات را دارا است.

اثربخشی پشتیبانی الکترونیکی

پشتیانی الکترونیکی به‌عنوان بخشی از فعالیت‌های جنگ الکترونیک تحت کنترل مستقیم فرمانده عملیات در پشتیبانی از فعالیت‌های شنود، شناسایی و تعیین محل منابع عمدی و غیرعمدی پرتوهای الکترومغناطیسی به کار گرفته می‌شود اهداف اقدامات پشتیبانی شامل شناسایی و تفسیر تهدیدهای آنی در آرایش الکترونیکی منطقه نبرد است. پشتیبانی الکترونیکی

می‌تواند سامانه‌های مخابراتی دشمن، همچنین سامانه‌های تهاجم الکترونیکی دشمن را شناسایی کند. امواج ساطع‌شده از جانب سامان‌های مخابراتی دشمن، به‌عنوان اولین نشانه‌های شناسایی برای پشتیبانی الکترونیکی باشد.

جستجو

فرآیند جستجو وظیفه شناسایی فعالیت‌های الکترونیکی در یک طیف الکترومغناطیسی و همچنین دسته‌بندی مخابرات ارسالی در داخل را بر عهده دارد گیرنده‌های جستجو باید برای شناسایی و عملکرد به‌موقع در طی ارسال در داخل میدان پوششی دشمن قرار گیرند. یک فرایند جستجو می‌تواند در هر یک از حوزه‌های مکان، زمان و فرکانس در نظر گرفته شود. عملکرد جستجو می‌تواند به‌صورت یک شناسایی عمومی و یا به‌صورت خاص برای یافتن نشانه‌های مخصوصی از صدا، نوع مدولاسیون و یا ویژگی‌های دیگری از سیگنال یا ترافیک باشد.

جهت‌یابی

جهت‌یابی اطلاعاتی را درباره جهت احتمالی یک ساطع کننده پرتوهای الکترومغناطیسی را فراهم می‌کند جهت‌یاب‌ها برای پیدا کردن موقعیت ساطع کننده‌ها، بر مبنی یک قانون مثلثی اقدام استوار است. دقت جهت‌یاب در طراحی صحنه الکترومغناطیس میدان رزم نقش اساس را ایفا می‌کند.

اثرپذیری شنود

مرحله‌ای که عمل شنود سیگنالی را آشکارسازی می‌کند آن را به گیرنده شنود انتقال داده تا بر اساس پارامترهایی مانند فرکانس، مدولاسیون و پهنای باند، سیگنال مربوطه را در طیف امواج الکترومغناطیسی طبقه‌بندی و در صورت امکان اطلاعات حاوی آن را استخراج کند این موضوع اغلب تحت عنوان شنود یا پایش بیان می‌شود. بعضی از ویژگی‌های سیگنال مانند فرکانس و پهنای باند، برای تعیین اهداف جنگ الکترونیک مناسب است.(عفیفی، احمد و همکاران-۱۳۸۵)

تأثیرات روی هدف

تأثیرات ممکن است در خودروی زرهی روی بخش کنترل خودرو، حسگرها و سامانه‌های جنگ‌افزاری به‌صورت ایجاد اختلال و یا آسیب دائمی به بخش‌های الکترونیکی باشد. زمان بازیابی در صورت ایجاد اختلال احتمالاً در سطح ثانیه است. آسیب دائمی به بخش‌های الکترونیکی ممکن است به‌صورت نابودی این بخش‌ها باشد و بازیابی آن نیاز به تعمیر خواهد داشت که ممکن است ساعت‌ها به طول انجامد. زمان بازیابی به هنگام ایجاد اختلال در سامانه‌های فرماندهی و کنترل یا تأسیسات لجستیکی احتمالاً در سطح دقیقه برای راه‌اندازی مجدد رایانه‌ها خواهد بود. بعضی از این اطلاعات ممکن است از بین برود ولی درصورتی‌که سامانه‌ها به‌دقت طراحی‌شده باشد تأثیر این اتلاف جزئی خواهد بود.

اثربخشی تهدیدات الکترونیکی غیر ارتباطی

آگاهی از موقعیت دشمن نیاز به برتری اطلاعاتی دارد. رشد سریع حسگرهایی زمینی، هوایی، دریای و فضایی، امکان انتشار اطلاعات را بیشتر و وسیع‌تر کرده است سامانه‌های موجود در فضا نیز به تسلط از طریق برتری اطلاعاتی کمک می‌کنند. تفکیک اطلاعات دریافتی از ماهواره‌های خودی، بی‌طرف و دشمن، در این زمینه نقش اساسی دارند اساس برتری اطلاعاتی مدیون سامانه‌ها و فناوری (سی- فور- آی)[1] است که می‌تواند برای کلیه سطوح فرماندهی یک تصویر عملیاتی قوی و مستمر از صحنه نبرد تهیه نماید. آگاهی از وضعیت دشمن همان عنصری است که می‌تواند تأثیر زیادی در انجام مأموریت فرماندهان داشته باشد.

اختلال رادار

در رادار جستجو معمولاً از اختلال نویز یا اختلال فریب استفاده می‌کنند، اما اغلب رادارها ردگیری می‌توانند اخلالگر نویزی را نیز تعقیب کنند بنابراین معمولاً از اختلال فریب برای شکستن قفل ردگیری استفاده می‌شود. اختلال فریب به انرژی کمتری نیاز دارد، درحالی‌که

[1] C4I:command,control,computer,communication,intelligence

اختلال نویزی در مقابل رادار ردگیری (به دلیل مکث زیاد و بهره آنتن بالا) احتیاج به توان فوق‌العاده زیادی دارد. اختلال هنگامی باعث آسیب زدن به اطلاعات رادار می‌گردد که نسبت سیگنال تداخلی (مثل نویز و اختلال) به سیگنال بازتابی از هدف در ورودی آشکارساز رادار، برابر یا بزرگ‌تر از ثابت اختلال گردد. ثابت اختلال به نوع و پارامترهای اختلال و سیگنال مفید و البته به نوع و قدرت رادار در آنالیز داده‌ها وابسته است. (جعفری، سید بهزاد و همکاران- ۱۳۹۲: ۷۱)

فریبنده‌های راداری

فریبنده‌های راداری درواقع اهداف کاذبی هستند که از دید رادار شبیه یک هدف واقعی به نظر می‌رسند و تنها برای فریب رادار دشمن به کار می‌رود. این نوع اهداف به‌گونه‌ای طراحی می‌شود که هدف شبیه سکوی موردحفاظت برای رادارهای دشمن ایجاد نماید. تفاوت میان فریبنده‌های راداری و انواع دیگر اخلالگر در این است که اهداف کاذب در کارکرد راداری که آن را ردگیری می‌کند تداخلی ایجاد نمی‌کند بلکه فقط درصدد جلب‌توجه رادار است و می‌خواهد رادارها آن را هدف‌یابی کنند. این نوع آفند از نوع فریب است. فریبنده‌های راداری: شامل ۱- فریبنده‌های راداری غیرفعال ۲- فریبنده‌های راداری آشکارساز ۳- فریبنده‌های راداری فعال است (واحدی، مرتضی و قیاسی، علی‌اکبر- ۱۳۹۰: ۱۱۴).

اختلال فریب

هدف اصلی اخلالگر فریب ارسال اطلاعات نادرست به سمت رادار با استفاده از سیگنال‌های مشابه به سیگنال مورد انتظار رادار است. با این تفاوت که توان بیشتر از سیگنال اصلی رادار است. این نوع تجهیزات قادرند سیگنال رادار را دریافت و ضبط نموده و در زمان مناسب با مدولاسیون‌های مناسب ازنظر دامنه، اختلاف‌فاز و پلاریزاسیون، مجدداً آن را برای رادار ارسال نمایند. اساساً اخلالگری فریب می‌تواند دارای انواع زیر باشد:

۱- ایجاد هدف‌های کاذب به‌صورت چندتایی جهت مقابله علیه رادارها تجسسی یا ردیاب در مرحله هدف‌یابی

۲- شکستن قفل ردیابی علیه رادار ردیاب با تغییر دادن برد رادار به سمت بردی نادرست

۳- فریب در سرعت علیه رادار ردیاب که از اثر دوپلر استفاده می‌کند.

۴) ایجاد اهداف کاذب با مدولاسیون دامنه علیه رادارهای ردیاب .(جعفری، سید بهزاد و همکاران-۱۳۹۲ :۶ ج۱).

شنود راداری

عنصر اول هر سامانه ضد الکترونیک را می‌توان گیرنده استراق سمع دانست. این گیرنده با انجام عمل شنود راداری سعی در استنتاج رادارهای موجود در محیط دارد. آن گیرنده‌ها به محدوده-ی وسیعی از فرکانس‌های رادیویی حساس هستند و از آنتن‌هایی استفاده می‌کنند که تقریباً از تمامی جهات سیگنال‌ها را دریافت می‌کنند همچنین پلاریزاسیون آنتن‌ها عموماً دایروی بوده تا پلاریزاسیون آنتن رادارها تأثیر چندانی در شنود سیگنال‌های آن‌ها نداشته باشد بدین ترتیب سعی می‌شود که حضور تمامی رادارهای تهدید برانگیز کشف شود مأموریت کسب اطلاعات راداری یک منطقه، بسته به اولویت زمان یا سرعت، بر عهده یکی از سامانه‌های اطلاعات الکترونیکی (الینت) گذاشته می‌شود(نصیر زاده، عزیز- شاه رضایی محمدحسن، ۱۳۹۱: ۵-۷)

اثربخشی مسینت‌ها

درواقع مسینت شامل اطلاعات علمی و فنی می‌گردد که از طریق تجزیه‌وتحلیل کیفی و کمی اطلاعات (مقیاس، زاویه مکانی طول‌موج، زمان، مدولاسیون، پلاسما، هیدرو مغناطیسی و...) توسط حسگرهای ویژه به کار می‌رود هدف این حسگرها، شناسایی هر نوع ویژگی مشخص است که مرتبط با منبع فرستنده یا ارسال‌کننده باشد و نیز تسریع در شناسایی و اندازه‌گیری‌های بعدی می‌باشند. در پشتیبانی از عملیات نظامی، از اثرات اطلاعات از طریق سنجش و علائم در افزایش دقت هدف‌گیری مهمات، تهیه مقدمات آگاهی و خبرگیری از مناطق عملیاتی، ارزیابی از ویرانی یا زیان‌های وارده در میدان نبرد، کنترل فضا، جستجو و نجات، شکار موشک‌های اسکاد و.... استفاده می‌شود مثلاً در عملیات طوفان صحرا، تحلیلگران اداره مرکزی اطلاعات سنجش و علائم آمریکا، محصولات اطلاعات از طریق حساسه‌های سنجش و علائم را خصوص موشک‌های اسکاد عراقی در عرض ۲ تا ۸ ساعت در اختیار نیروهای ذینفع متحد قرار می‌داد. اطلاعات سنجش و علائم، سامانه‌های تسلیحات هسته‌ای، شیمیایی بیولوژیکی و سایر تسلیحات پیشرفته متعارف را شناسایی و ره‌گیری می‌کند. اطلاعات سنجش و علائم هدف را از یک‌فاصله امن و بر اساس مشخصاتی از هدف (مثل: دود راکت و ترکیبات

بیولوژیکی و مولکولی) آشکار می‌نماید. جزئیات این قابلیت‌ها به‌صورت اطلاعات طبقه‌بندی‌شده است. اما روش‌های پردازشی مثل تصویرسازی حرارتی چند طیفی، دید وسیعی در دنبال کردن تشعشعات گازی (مثل تشعشعاتی که از تسلیحات هسته‌ای یا شیمی‌ای ساطع می‌شود) ارائه می‌دهد مدل‌های فرآیند اطلاعات سنجش و علائم شامل دمای سطحی، کیفیت آب، ترکیبات ماده‌ای و آلاینده‌ها است.

ملاحظات در اثربخشی یک سامانه فرماندهی و کنترل

یکی از عوامل کیفی در اندازه‌گیری اثربخشی سامانه (سی- فور- آی)، وسعت فرماندهی و کنترل در تصمیم‌گیری است. این عامل سرعت شامل ورود اطلاعات، تحلیل، تصمیم‌گیری و دیگر اقدامات مربوطه می‌گردد. در اینجا سرعت عملکرد سامانه‌های رایانه‌ای و مخابراتی در ارسال اطلاعات و سرعت عمل فرماندهی در تصمیم‌گیری، باهم ترکیب‌شده و کیفیت عامل سرعت در سامانه را تعیین می‌کند. عامل دیگری که در ارزیابی کیفیت سامانه موردنظر است تغذیه‌ای اطلاعات به سامانه‌های پشتیبان مدیریت سامانه و توزیع نتایج آن در اسرع وقت و با روشی مطمئن و ایمن، در بین عناصر تصمیم‌ساز و تصمیم‌گیرنده سامانه است عوامل فوق ازجمله معیارهای تعیین‌کننده در ارزیابی کیفیت تبدیل داده‌ها و ارزش اطلاعات آن‌ها به شمار می‌رود که به سهم خود یکی دیگر از شاخص‌های ارزیابی اثربخشی سامانه است. (نصیر زاده، عزیز- شاه رضایی محمدحسن ۱۳۹۱: ۲۳۷)

روش‌شناسی پژوهش

تحقیق حاضر از حیث روش توصیفی-تحلیلی و ازلحاظ هدف کاربردی است. برای جمع‌آوری اطلاعات و داده‌های موردنیاز از بررسی‌های اسنادی و کتابخانه‌ای و مطالعات میدانی استفاده می‌شود. علاوه بر توزیع پرسشنامه و تحلیل آن، میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا شناسایی و مورد تحلیل قرارگرفته است. جامعه موردمطالعه فرماندهان گروه ۴۰۲ جنگال نزاجا در رده‌های مختلف (دسته به بالا)، جامعه موردمطالعه است. برای تعیین حجم نمونه از تخمین فاصله‌ای میانگین استفاده شد که درنهایت ۵۸ نفر از کارکنان مذکور به‌عنوان حجم نمونه انتخاب شدند.

$$n=\frac{N(Z_a/2)^2\times\sigma^2}{D(N-1)+(Z_a/2)^2\times\sigma^2}=\frac{320(1.96)^2\times3.7}{0.2(320-1)+(1.96)^2 3.7}=\frac{4548.48}{78.01}=58.3\approx58$$

Z_a با ضریب اطمینان ۹۸٪ از طریق جدول مربوطه محاسبه‌شده است. واریانس جامعه آماری از روی تحقیق انجام‌گرفته شده از قبل در این شرکت تعیین‌شده است. با توجه به این‌که جامعه آماری این تحقیق از طبقات مختلف (افسران ارشد ، افسران جزء درجه‌داران و کارمندان) تشکیل‌شده است جهت اینکه حجم نمونه نماینده واقعی جامعه آماری باشد به‌صورت تصادفی طبقاتی انتخاب‌شده است. برای تعیین روایی پرسشنامه، پرسشنامه به تعداد کافی در اختیار اساتید و متخصصان در هر حوزه قرار گرفت و پس از بررسی‌های لازم و حذف تعدادی از سؤالات پرسشنامه ازنظر روایی مورد تأیید قرار گرفت. برای تعیین پایایی پرسشنامه در مرحله پیش‌آزمون از آلفای کرون باخ استفاده شد که عدد ۰/۸۴۷ به دست آمد، بنابراین پایایی پرسشنامه در حد عالی ارزیابی می‌شود.

تجزیه‌وتحلیل یافته‌های پژوهش

فرضیه تحقیق: به نظر می‌رسد بررسی میزان تأثیر تهدیدات الکترونیکی نیروی خودی بر سامانه‌های الکترونیکی (ارتباطی و غیر ارتباطی)نیروی دشمن، بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا در نبرد ناهمتراز، تأثیر زیادی خواهد داشت.

برمبنای جدول تجزیه‌وتحلیل توصیفی فرضیه اول می‌توان میانگین و واریانس داده‌های فوق را به‌صورت زیر محاسبه کرد:

میانگین:

$$\overline{X}=\frac{\sum_{i=1}^{k} f_i x_i}{n}=\frac{259}{58}=4/46$$

واریانس:

$$S^2=\frac{\sum_{i=1}^{N} f_i(x_i-\bar{x})^2}{n-1}=\frac{28/42}{57}=0/50$$

انحراف معیار:

$$S=\sqrt{S^2}=0/70$$

۹۱ درصد از جامعه نمونه معتقدند بررسی میزان تأثیر تهدیدات الکترونیکی نیروی خودی بر سامانه‌های الکترونیکی (ارتباطی و غیر ارتباطی)نیروی دشمن ، بر فرآیند تصمیم‌گیری عملیات

جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا در نبرد ناهمتراز تأثیر زیادی خواهد داشت و این میزان تأثیر (با توجه به میانگین به‌دست‌آمده یعنی (۴/۴۶) را در حد زیاد و بالاتر دانسته‌اند.

در این تحقیق، فرآیند تصمیم‌گیری عملیات جنگ الکترونیک، با استفاده از اسناد و مدارک و مصاحبه با صاحب‌نظران احصا گردید و در تحلیل کمی نیز میزان تأثیر تهدیدات الکترونیکی خودی بر سامانه‌های ارتباطی و غیر ارتباطی دشمن بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا در نبرد ناهمتراز بررسی گردید.

برای بررسی عوامل مؤثر بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا، تعداد ۱۲سؤال برای جامعه نمونه مطرح شد که به‌منظور تجزیه‌وتحلیل و مشخص ساختن اطلاعات به‌دست‌آمده، پاسخ پرسش‌شوندگان موردمطالعه و بررسی قرار گرفت و شاخص‌ها مشخص گردید. سپس میانگین تأثیر شاخص‌ها از طریق جداول، مشخص و میانگین و واریانس داده‌ها محاسبه گردید و با استفاده از جدول خی ۲ مقدار بحرانی، آماره آزمون و فرضیه صفر، رد و فرضیه ادعا اثبات شد. برای فرضیه تحقیق، شدت تأثیر تهدیدات الکترونیکی نیروهای خودی بر سامانه‌های ارتباطی و غیر ارتباطی دشمن ، بر فرآیند تصمیم‌گیری عملیات جنگ الکترونیک گروه ۴۰۲ جنگال نزاجا درنبرد ناهمتراز به میزان ٪۶۷ به دست آمد. که این موضوع اثبات می‌نماید، متغیرهای در نظر گرفته‌شده برای هرکدام از فرضیه‌ها از یکدیگر مستقل نبوده و بین آن‌ها ارتباط معناداری وجود دارد و بر همدیگر تأثیر دارند.

نتیجه‌گیری و پیشنهادها

نتایج تحقیق نشان داد که کسب اطلاعات الکترونیکی صحنه نبرد، اطلاعات فنی سامانه‌ها و تجهیزات جنگ الکترونیک دشمن و سامانه‌های هدف، ارتقا، بهبود یا اصلاح اقدام جمع‌آوری اخبار الکترونیکی، پردازش و تجزیه‌وتحلیل تهدیدات الکترونیکی، بررسی میزان تأثیر تهدیدات الکترونیکی خودی(اختلال، فریب، رمزگشایی، ره‌گیری، شنود و...) بر سامانه‌های ارتباطی دشمن، بررسی میزان تأثیر تهدیدات الکترونیکی غیر ارتباطی خودی(اختلال راداری، فریب راداری، فریبنده‌های راداری، دکوی، شنود راداری، اطلاعات علمی و فنی مسینت‌ها، پنهان نگاری و اختلال ماهواره‌ای، اختلال سایبری) بر سامانه‌های الکترونیکی دشمن، افزایش توانمندی نیروی انسانی، تجهیزات و ساختارها، بر فرآیند تصمیم‌گیری عملیات جنگال گروه ۴۰۲ جنگال در نبرد ناهمتراز تأثیر زیادی خواهد نمود.

پیشنهادها

الف) تدابیر لازم مبتنی بر مطالعه روندهای اخیر و آینده‌پژوهی تهدیدات و محیط جنگ آینده اخذ و آموزش‌ها و سازمان‌دهی مناسب داده شود و همچنین سامانه‌های تهدیدشناسی ، واحدهای تجزیه‌وتحلیل و طرح‌ریزی عملیات جنگال، تقویت گردند.

ب) نسبت به اصلاح فرآیند تصمیم سازی و تصمیم‌گیری عملیات جنگال اقدام گردد.

پ) رسد کنترل عملیات در خصوص بازخورد گیری به‌موقع و صحیح از عملیات جنگال اقدام نماید.

ت) نسبت به افزایش دانش مدیریتی فرماندهان و مسئولان در چرخه فرماندهی و کنترل عملیات جنگال با برگزاری دوره‌های مرتبط در مراکز علمی و دانشگاهی اقدام گردد.

ث) نسبت به طراحی و راه‌اندازی سامانه بازی جنگ عملیات جنگال و شبیه‌سازهای تجهیزات جنگال و آزمایشگاه‌های سیگنال و آنتن در مراکز آموزش تخصصی جنگال آجا، اقدام گردد.

ج) نسبت به اعزام تعدادی از فرماندهان و مدیران جنگال به کشورهای دوست و هم‌پیمان جهت فراگیری و تبادل تجربیات آموزشی، در دوره‌های آموزشی طرح‌ریزی عملیات جنگال، بازی جنگ عملیات جنگال، مدیریت فناوری اطلاعات و مدیریت بحران الکترونیکی و... اقدام گردد.

منابع

- اصغری، غلامعلی (۱۳۹۳)، *دفاع الکترونیک ویژه مرکز آموزش مخابرات*، چاپ اول، تهران، انتشارات مرآمخ نزاجا
- الوانی، سید مهدی (۱۳۹۱)، *مدیریت عمومی*، چاپ دهم، تهران، انتشارات سمت
- حمیدی، محمدرضا (۱۳۸۷)، *تصمیم‌گیری نوین*، چاپ اول، تهران، نشر دانشگاه دفاع ملی
- ستاری‌خواه، علی؛ مسلمی، حسین (۱۳۹۳)، *عملیات طرح‌ریزی پدافند الکترونیکی و سایبری*، تهران، انتشارات دافوس آجا
- شیخ، محمدرضا و همکاران، (۱۳۹۷)، *جنگ ناهمتراز*، چاپ اول، تهران، نشر دانشگاه فرماندهی و ستاد آجا

- گودرزی، محمدعلی و همکاران (۱۳۹۸)، *مهارت‌های مسئله یابی و تصمیم‌گیری*، چاپ دوازدهم، تهران، انتشارات دانشگاه پیام نور
- محمدی محمود و همکاران، (۱۳۸۵)، *نقش فناوری اطلاعات در جنگ‌های آینده (جلد اول)*، چاپ اول، تهران، انتشارات موسسه آموزشی و تحقیقاتی صنایع دفاعی
- مسلمی، حسین (۱۳۹۴)، *تدوین راهبردهای فرماندهی جنگال راهبردی ارتش جمهوری اسلامی ایران*، رساله دکتری، دانشگاه عالی دفاع ملی، تهران
- نباتی، عزت اله، (۱۳۹۱)، *جنگ الکترونیک*، چاپ اول، تهران، انتشارات مرکز آموزشی و پژوهشی شهید صیاد شیرازی
- نصیر زاده، عزیز؛ شاه‌رضایی، محمدحسن (۱۳۹۱)، *میدان نبرد دیجیتال*، چاپ اول، تهران، انتشارات مرکز آموزش شهید سپهبد صیاد شیرازی تهران
- واحدی، مرتضی، (۱۳۹۰)، *کلیات جنگ الکترونیک*، چاپ اول، تهران، انتشارات دانشکده علوم و فنون دارابی
- ولی‌وند زمانی، حسین، و همکاران،(۱۳۹۸)، *تصمیم سازی و تصمیم‌گیری در محیط نظامی*، چاپ دوم، تهران، نشر دانشگاه فرماندهی و ستاد آجا

- FM3-12, *Cyberspace and electronic warfare operations*, headquarters, department of the arm, 2017
- FM3-36, *Electronic warfare*, headquarters, department of the army, 2012
- FM5-0c1,*the operation process*, Washington DC,2012