فصلنامه علمی – پژوهشی فرماندهی و کنترل،سال سوم، شماره دو،تابستان۱۳۹۸

مناسب‌ترین راهبردهای پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل در برابرتهدیدهای شنود الکترونیکی توسط حساسه‌های اطلاعات ارتباطی دشمن

دکتر محمد سپهری[۱]

تاریخ دریافت: ۱۳۹۸/۰۳/۱٦ تاریخ پذیرش: ۱۳۹۸/۰٦/۱۲

چکیده

ارتباط و رایانه دو فناوری مهم و تعیین کننده در سامانه فرماندهی و کنترل است که وظیفهٔ پشتیبانی از مؤلفه‌های فرماندهی و کنترل، اطلاعات، عملیات مراقبت و عملیات شناسایی را به عهده دارند. دشمن با استفاده از بکارگیری حساسه‌های پیشرفته اطلاعات ارتباطی(کامینت) از زمین، دریا، فضا، هوا و فضای سایبری کلیه فعالیت‌ها و ارتباط‌های سامانه‌های ارتباطی و سایبری مورد استفاده در شبکه‌های فرماندهی و کنترل کشورمان را رهگیری، موقعیت‌یابی و شناسایی می‌نماید. مساله اصلی تحقیق؛ مُدّون نبودن راهبردهای پدافند غیرعامل ارتباطی سامانه‌های ارتباطی کشور در برابر تهدیدهای رهگیری و شناسایی توسط حساسه‌های اطلاعات ارتباطی دشمن می‌باشد. بنابراین پدافند غیرعامل ارتباطی با هدف افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی، تسهیل مدیریت بحران و مصون‌سازی سامانه‌های ارتباطی و سایبری در شبکه فرماندهی و کنترل یکی از بهترین راه‌های مقابله با تهدیدات و اقدامات رهگیری، موقعیت‌یابی و شناسایی سامانه‌های ارتباطی و سایبری توسط حساسه‌های اطلاعات ارتباطی دشمن می‌باشد. مقاله حاضر پس از ارائه مطالبی مربوط به تهدیدهای مختلف برعلیه سامانه‌های ارتباطی مورد استفاده در شبکه فرماندهی و کنترل به بررسی عملکرد پدافند غیرعامل ارتباطی و راهبردهای مقابله با تهدیدهای حساسه‌های اطلاعات ارتباطی می‌پردازد. این پژوهش کاربردی و توسعه‌ای، روش تحقیق آمیخته از نوع موردی- زمینه‌ای، روش گردآوری اطلاعات اسنادی و پیمایشی و ابزار آن مصاحبه و جامعه آماری ٦۰ نفر می‌باشد که با استفاده از ماتریسSWOT جهت تجزیه و تحلیل محیط داخل و خارج و تدوین راهبردها و از نرم‌افزار TOPSIS در تعیین اولویت راهبردهای پدافند غیرعامل ارتباطی کشور در مقابله با تهدیدهای مختلف حساسه‌های اطلاعات ارتباطی دشمن استفاده گردید.

واژه‌گان کلیدی: پدافند غیرعامل، فرماندهی و کنترل، اطلاعات ارتباطی، شنود الکترونیکی.

[۱]- استادیار – عضو هیئت علمی دانشگاه پدافند هوایی خاتم الانبیاء(ص)- SEPEHRI377 @CHMAIL.IR .

۱- کلیات

۱-۱-مقدمه

دشمن[1] با اهداف خاص نظامی، امنیتی، اطلاعاتی و اقتصادی کار جمع‌آوری اطلاعات، مراقبت و شناسایی[2] از سامانه‌های ارتباطی و سایبری شبکه فرماندهی و کنترل ما را با استفاده از بکارگیری حساسه‌های مختلف جمع‌آوری اطلاعات به خصوص حساسه‌های اطلاعات سیگنالی[3] در دو بخش حساسه‌های اطلاعات ارتباطی(کامینت)[4] و حساسه‌های اطلاعات الکترونیکی(الینت)[5] از زمین، دریا، هوا، فضا و فضای سایبری و از طریق کشورهای همسایه‌ی ایران اقدام به جمع‌آوری اطلاعات راه‌کنشی، عملیاتی و راهبردی می‌نماید. از مهمترین تهدیدهای برعلیه سامانه‌های ارتباطی و سایبری ما رهگیری، موقعیت‌یابی و شناسایی توسط حساسه‌های حساسه‌های اطلاعات ارتباطی می‌باشد. اقدامات پدافند غیرعامل ارتباطی مهمترین گام در کاهش، عدم رهگیری، گمراه‌سازی و خنثی‌سازی تهدیدهای حساسه‌های اطلاعات ارتباطی آمریکا می‌باشد. بنابراین به منظور افزایش بازدارندگی، کاهش آسیب‌پذیری و مصون‌سازی در طیف فرکانس رادیویی در مقابل تهدیدات و اقدامات جمع‌آوری اطلاعات توسط حساسه‌های اطلاعات ارتباطی دشمن، اقدامات پدافند غیرعامل ارتباطی امری لازم و ضروی می‌باشد که به دلیل عدم تدوین راهبردهای این حوزه بنابراین دغدغه و مشکلی اساسی" **مُدّون نبودن راهبردهای پدافند غیرعامل ارتباطی سامانه‌های ارتباطی کشور در برابر تهدیدهای رهگیری و شناسایی توسط حساسه‌های اطلاعات ارتباطی دشمن**" به عنوان مسئله اصلی تحقیق می‌باشد. بنابراین شناخت نقاط قوت، ضعف، فرصت و تهدید پدافند غیرعامل ارتباطی به منظور کاهش و دفع تهدیدهای حساسه‌های اطلاعات ارتباطی آمریکا با بکارگیری اقدامات پدافند غیرعامل ارتباطی امری لازم و ضروری می‌باشد و در صورت عدم شناخت کامل تهدیدهای موجب غافل‌گیری راهبردی، رهگیری، کشف و شناسایی بسیار آسان توسط حساسه‌های اطلاعات ارتباطی آمریکا و بالا رفتن هزینه‌های دفاعی، ضربه خوردن از نقاط آسیب‌پذیر در سامانه‌های ارتباطی در سامانه‌های فرماندهی و کنترل می‌گردیم.

۱-۲-سوال اصلی تحقیق:

راهبردهای پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل کشور در برابر تهدیدهای رهگیری، موقعیت‌یابی و شناسایی توسط حساسه‌های اطلاعات ارتباطی دشمن چیست؟

۱-۳- هدف اصلی تحقیق:

تدوین راهبردهای پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل کشور در مقابله با تهدیدهای رهگیری، موقعیت‌یابی و شناسایی توسط حساسه‌های اطلاعات ارتباطی دشمن.

۲- مبانی نظری

2-1- پیشینه تحقیق

مشابه موضوع مقاله‌ی مذکور در دانشگاه‌های داخل و خارج کشور انجام نشده است، ولی عناوین رساله‌ها، تحقیات و مقالات مرتبط با متغیرهای مورد نظر در مقاله مذکور عبارتند از:

(۱)- پروژه تحقیقاتی"بررسی تطبیقی پایش تهدیدات فناوری‌های اطلاعات شناسایی و الکترونیک هوایی آمریکا و ترازیابی توان فناوری‌های اطلاعات شناسایی و الکترونیک هوایی ایران و آمریکا " با هدف اصلی تحقیق، الگوی تحلیلی مناسب جهت مقابله با تهدیدهای حوزه اطلاعات هوایی، که مهمترین نتایج حاصله عبارتند از؛ بهره‌گیری از توان صنایع مرتبط در ایجاد اختلال در رایانه‌های دشمن از طریق سوابق اطلاعاتی و تهیه نرم‌افزار رایانه‌ای، استفاده جهت‌دار دانش نخبگان به منظور شناسایی حساسه‌های سنجشی و علائمی[6] و جنگ اطلاعات، بهره‌گیری از توان علمی نخبگان به منظور ایجاد اختلال در بکارگیری رایانه توسط دشمن و کاهش کارایی و عدم دسترسی او به اطلاعات در عمق کشور از طریق تهیه نرم‌افزارها، بکارگیری تجربه نسبتا بالای جمع‌آوری اطلاعات به منظور محدود نمودن دسترسی دشمن به اطلاعات تاکتیکی از طریق سوابق موجود، تقویت آموزش اطلاعات به منظور دریافت تاکتیک‌های ضدشنود دشمن، بکارگیری توان رهگیری مستمر

۱- در مقاله منظور از دشمن، فقط تهدیدهای شنود الکترونیکی توسط حساسه‌های اطلاعات ارتباطی(کامینت) آمریکا می‌باشد.

2 - INFORMATION SURVEILLANCE RECONNAISSANCE (ISR)

3 -SIGNAL INTELLIGENCE (SIGINT)

4 - COMMUNICATION INTELLIGENCE (COMINT)

5 -ELECTRONIC INTELLIGENCE (ELINT)

6 -Measurment And Signature Intelligence(MASINT)

اطلاعات و تجربه بالای جمع‌آوری اطلاعات، ایجاد هماهنگی‌های موثر درون سازمانی و برون سازمانی و همچنین اصلاح مدیریت اطلاعات به منظور کاهش دسترسی دشمن به اطلاعات تاکتیکی و راهبردی در عمق از طریق تشکیل کار گروه‌های تخصصی، بکارگیری قابلیت‌های صنایع در ارسال اطلاعات مجازی به منظور اشباع شبکه اطلاعاتی دشمن او از طریق نفوذگرها.[1]

(۲)- پروژه تحقیقاتی"جمع‌آوری، تحلیل و پردازش اطلاعات سامانه‌های جنگ الکترونیک ارتش آمریکا مستقر در خلیج فارس" با هدف اصلی، ارائه اطلاعات سامانه‌های جنگ الکترونیک و اطلاعات ارتباطی یگان‌های ارتش آمریکا مستقر در منطقه خلیج فارس در سه سطح راه‌کنشی، عملیاتی و راهبردی، که مهمترین نتایج حاصله عبارتند از؛ کوچک و کیفی‌سازی سازمان اطلاعات ارتباطی و جنگ الکترونیک، تجهیز و آماده‌سازی در رده‌های کوچک‌تر، برخورداری از ساختار تجزیه و تحلیل منسجم و مستقل و منطبق با مقدورات و توانمندی‌های هر سازمان و اتصال آن به شبکه عملیاتی و غیرعملیاتی، برخورداری از فناوری مخابراتی منطبق با استانداردهای جهانی و اتصال امن و غیرقابل اختلال و رهگیری مراکز جمع‌آوری اطلاعات منطقه‌ای و فرامنطقه‌ای، برخورداری از تجهیزات اطلاعات ارتباطی و جنگ الکترونیک چند منظوره‌ی کم حجم با قابلیت تحرک‌پذیری و کنترل از راه دور، ارتباط نیروهای عملیاتی با مراکز فرماندهی و کنترل، قابلیت استقرار و ایجاد ارتباط نیروی واکنش سریع، دگرگونی در سامانه‌ها، کاهش وزن و اندازه تجهیزات توسط آمریکا می‌باشد.[2]

(۳)- رساله دکتری"تدوین راهبرد ملی پدافند غیرعامل در حوزه ارتباطات" که راهبردهای بهینه پدافند غیرعامل کشور عبارتند از؛ توسعه ساختارهای مدیریتی و عملیاتی فعال پدافند غیرعامل در کلیه رده‌های سازمانی، تعمیم فناوری پدافند غیرعامل در کلیه ساختارها و لایه‌های سازمانی، بومی‌سازی و انتقال دانش و فناوری ارتباطات و اطلاع‌رسانی بداخل کشور، ایمن‌سازی زیرساخت‌ها و مراکز حساس ارتباطی و اطلاع رسانی می‌باشد.[3]

(٤)- رساله دکتری"راهبردهای پدافند غیرعامل سامانه‌های راداری و ارتباطی آجا در برابر تهدیدات ناهمتراز از ناحیه حساسه‌های اطلاعات سیگنالی دشمن" که راهبرهای؛ فریب، کمک به بازدارندگی، کاهش آسیب‌پذیری و مصون‌سازی، چابکی، کنترل و پاسخگویی در برابر تهدیدات، ارتقاء پایداری ملی، ارتقاء سطح آمادگی، محروم‌سازی دشمن و هشداردهی در برابر تهدیدات و اقدامات دشمن احصاء گردید. [4]

(۵)-مقاله"راهبردهای پدافند غیرعامل الکترونیک آجا در برابر تهدیدات ناهمتراز حساسه‌های اطلاعات سیگنالی دشمن" آمریکا با بکارگیری حساسه‌های پیشرفته اطلاعات سیگنالی در پایگاه‌های مختلف نظامی از هوا، فضا، زمین، دریا و فضای سایبری در همسایگی ایران کلیه فعالیت‌های سامانه‌های راداری، ارتباطی و سایبری کشور ما را رهگیری و شناسایی می‌نماید. پدافندغیرعامل الکترونیک با هدف افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی، تسهیل مدیریت بحران و مصون‌سازی سامانه‌های راداری و ارتباطی یکی از مناسب‌ترین راه‌های مقابله با تهدیدات و اقدامات حساسه‌های اطلاعات سیگنالی دشمن می‌باشد. که در این مقاله پس از ارائه مطالبی مربوط به تهدیدات حساسه‌های اطلاعات سیگنالی به بررسی عملکرد پدافند غیرعامل الکترونیک(ارتباطی و راداری) می‌پردازد. و در نهایت راهبردهای پدافند غیرعامل الکترونیک آجا در مقابله با تهدیدات ناهمتراز حساسه‌های اطلاعات سیگنالی دشمن ارائه می‌نماید.[5]

(٦)-مقاله"امنیت فضای تبادل اطلاعات کشور، پیش‌نیاز و حافظ اقتدار ملی امنیت فضای تبادل اطلاعات(افتا)"با هدف ضرورت پرداختن و نقش امنیت فضای تبادل اطلاعات در ارتباط با اقتدار ملی می‌باشد که مهمترین نتایج حاصله عبارتند از؛ اقتدار پایدار نیازمند توسعه و توسعه شامل فضای تبادل اطلاعات می‌باشد و اقتدار نیازمند حافظ و امنیت فضای تبادل اطلاعات هم یک حافظ، امنیت ملی بدون امنیت فضای تبادل اطلاعات ناممکن است. فضای تبادل اطلاعات نیازمند امنیت می‌باشد.[6]

2-2- مفهوم‌شناسی

(۱)- پدافند غیرعامل؛ مجموعه اقدامات غیرمسلحانه که موجب، افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد.[7]

(۲)- اطلاعات سیگنالی؛ جمع‌آوری اطلاعات از انتشارات الکترومغناطیسی دشمن، رقیب و دوستان در زمان صلح، بحران و جنگ از طریق جستجو، رهگیری، شناسایی، پیاده‌سازی و

موقعیت‌یابی منبع انتشار انرژی و امواج الکترومغناطیسی است که از بخش‌های اطلاعات الکترونیکی(الینت) و اطلاعات ارتباطی(کامینت) تشکیل شده است.[8]

(۳)-اطلاعات ارتباطی؛ از شنود پیام، پردازش و گزارش ارتباطات شبکه ارتباطی دشمن می‌باشد. ارتباطات در این عرصه به معنی صداها و داده‌ها، ارسال نمابر، پیام‌های اینترنتی و هر پیام عمدی قابل ارسال می‌باشد. اطلاعات ارتباطی توسط ماهواره‌ها و هواپیمای باسرنشین و بدون سرنشین، سایت‌های آشکار و پنهان زمینی و دریایی جمع‌آوری می‌گردد.[9]

(٤)-پدافند غیرعامل ارتباطی: اتخاذ روش‌های مناسب، موثر و قابل اجرا به منظور افزایش امنیت، ایمنی و پایداری سامانه‌های ارتباطی، غیرارتباطی (راداری) و سایبری در مقابل حملات ارتباطی، الکترونیکی و سایبری، عملیات شناسایی و جمع‌آوری اطلاعات ارتباطی(کامینت) دشمن، حذف یا به حداقل رساندن خسارات وارده به توانایی‌های نیروی انسانی، تجهیزات و سامانه‌های ارتباطی در مقابل اقدامات جمع‌آوری حساسه‌های طیفی، حملات وسیع تجهیزات تخریب الکترومغناطیسی و سایر سامانه‌های مرتبط دشمن با اجرای اصول پدافند غیرعامل می‌باشد.[10]

اتخاذ روش مناسب و موثر و قابل اجراء به منظور ارتقاء امنیت، ایمنی و پایداری ارتباطات به طوری که علی‌رغم حملات الکترونیکی و پشتیبانی الکترونیکی دشمن در استفاده موثر و مطلوب از طیف امواج رادیویی خودی را برای نیروهای خودی میسر می‌کند.[11]

(۵)- فرماندهی و کنترل؛ استفاده از منابع در دسترس، طرح‌ریزی به کارگیری، سازماندهی، هدایت، هماهنگی و کنترل نیروهای نظامی به منظور اجرای ماموریت‌های واگذاری که می‌تواند حفظ سلامت، رفاه، روحیه و انضباط کارکنان واگذار شده نیز باشد.[12]

۳-۲- ادبیات تحقیق

الف- پدافند غیرعامل در اسناد بالادستی

مقام معظم رهبری(مدظله‌العالی)می‌فرمایند: پدافند غیرعامل مثل مصونیت‌سازی برای بدن انسان است، از درون ما را مصون می‌کند. این معنایش این است که ولو دشمن تهاجمی بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد این پدافند غیرعامل نتیجه‌اش این است...ببینید چقدر مهم است که ما این حالت را برای کل پیکره کشور و جامعه در دستگاه‌های مختلف بوجود بیاوریم...کاری کنیم که مصونیت در خودمان بوجود بیاوریم، این با پدافند غیرعامل تحقق پیدا می‌کند. بنابراین این مسئله، مسئله بسیار مهمی است که بایستی راه بیفتد...بنابراین، پدافند غیرعامل یک اصل خواهد بود برای همیشه، نه برای یک مقطع خاص. [13]. پدافند غیرعامل بطور مستقیم و غیرمستقیم در اسناد بالادستی مانند؛ منابع‌دینی، فرمایشات و سخنان حضرت امام خمینی(ره)و فرماندهی معظم کل قوا، قانون اساسی، سند چشم‌انداز، سیاست‌های کلی نظام، برنامه چهارم، پنجم، ششم توسعه و سند راهبردی پدفند غیرعامل الکترونیک با نگاه دفاع همه جانبه از زیرساخت‌های حیاتی، حساس و مهم (سامانه‌های ارتباطی) کشور در کلیه برنامه‌ها و فعالیت‌ها با رعایت اصول و الزامات پدافند غیرعامل (ارتباطی) موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران و مصون‌سازی در مقابل تهدیدهای حساسه‌های اطلاعات ارتباطی و اقدامات نظامی دشمن می‌شود. ارتقاء مؤلفه‌های اصلی پدافند غیرعامل نیاز به بومی‌سازی، هوشمندسازی، مصون‌سازی فناوری‌های نوین سامانه‌های دفاعی به ویژه سامانه‌های الکترونیکی(راداری و ارتباطی)، هوافضایی، دریایی و پدافند هوایی می‌باشد. [14]فرهنگ‌سازی و ارتقاء سطح آموزش، تحقیقات و فناوری‌های پدافندغیرعامل نیاز به گسترش همکاری‌ها با مراکز علمی دانشگاهی نظامی و غیرنظامی کشور می‌باشد.[15] برنامه‌ریزی و هدایت پدافند غیرعامل الکترونیک با هدف مصون‌سازی، تضمین تداوم و راهبری ماموریت‌های؛ رصد، پایش، تشخیص، واپایش و هشداردهی تهدیدهای حوزه الکترونیک، مصون‌سازی و کاهش آسیب‌پذیری‌های زیرساخت‌های الکترونیک کشور در برابر تهدیدهای، گفتمان و فرهنگ‌سازی، تربیت نیروی انسانی مبتکر، متخصص و متعهد، طرح‌ریزی، آموزش، تجهیز، تمرین، رزمایش و ارزیابی برای ارتقاء آمادگی، طبقه‌بندی و سطح‌بندی زیرساخت‌ها بر اساس اهمیت و ماهیت، ساماندهی، راهبری و حمایت از تحقیق، توسعه و مدیریت دانش کارآمد، در پدافند غیرعامل الکترونیک و

ممانعت از دسترسی و بهره‌برداری دشمن از طیف الکترومغناطیس کشور می‌باشد.[16]

ب- توانمندی‌ها و تهدیدهای حساسه‌های اطلاعات ارتباطی(کامینت) آمریکا

• توانایی تعیین نوع، تعداد، تنوع، موقعیت، تحرک، جابجایی، اهداف، قابلیت‌ها، توانایی‌ها، نقاط قوت، نقاط ضعف، پیش‌بینی حمله قریب‌الوقوع، الگوی فعالیت هر فرستنده، تکنیک و تاکتیک‌های بکار گرفته‌شده و تعیین آرایش نظامی الکترونیکی سامانه‌های ارتباطی.[17]

• رهگیری، تجزیه و تحلیل و شناسایی و رمزگشایی کلیه ارتباطات توسط حساسه‌های اطلاعات ارتباطی از زمین، هوا، دریا، فضا و فضای سایبری.[18]

• تسلط کامل بر طیف فرکانس ارتباطی با بکارگیری انواع حساسه‌ها اطلاعات ارتباطی.

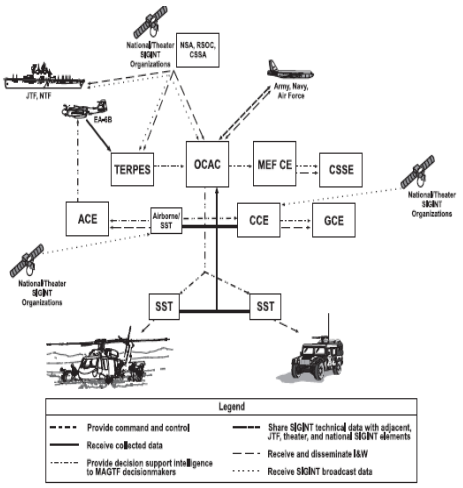
• پشتیبانی جامع شانزده سازمان تولید کننده اطلاعات ارتباطی از فرماندهان نظامی آمریکا.

• تهیه و تأمین اطلاعات ارتباطی در سه سطح راهکنشی، عملیاتی و راهبردی.

• استفاده بیش از ٦٥ پایگاه جمع‌آوری اطلاعات سیگنالی از زمین، دریا، هوا، فضا و فضای سایبری توسط آمریکا درهمسایگی ایران.

• جمع‌آوری هوشمند توسط حساسه‌های اطلاعات ارتباطی در عملیات راهکنشی، عملیاتی[1] و راهبردی از زمین، دریا، هوا، فضا و فضای سایبری‌از طریق کشورهای همسایه ایران.

• جمع‌آوری اطلاعات ارتباطی توسط حساسه‌های اطلاعات ارتباطی در حوزه‌های راهکنشی، عملیاتی و راهبردی توسط سازمان‌های و جامعه اطلاعاتی آمریکا (سازمان امنیّت ملی، آژانس اطلاعات دفاعی، آژانس اطلاعات فضایی، اداره شناسایی ملی، مراکز ذخیره اطلاعات مشترک، فرماندهی امنیت و اطلاعات نیروهای مسلح، آژانس امنیت ملی) و شبکه جمع‌آوری اشلون و پریزم.



شکل۱- معماری سامانه جمع‌آوری اطلاعات اشلون و اطلاعات سیگنالی امریکا

• استفاده از حساسه‌های اطلاعات ارتباطی هواپایه راهکنشی، عملیاتی و راهبردی (هواپیماهای JSTARS،GR/CS،U2، RC-۱۳۵ و RC-۱۳۵V، EC-۱۳۰، SR -۷۱، و TR -۱، RU-21H و RC-12D و پهپادهای گلوبال‌هاوک، ورهیت، شَدو[2] و بالون‌های پی‌اس‌اس‌تو[3] جمع‌آوری اطلاعات سیگنالی)

• استفاده بیش از ۲۰۰ ماهواره اطلاعات سیگنالی توسط سازمان امنیت ملی.[19]

• استفاده از حساسه‌های اطلاعات ارتباطی دریا پایه سطحی و زیرسطحی(توسط ناوهای هواپیمابر و بالگردان‌بر و زیرسطحی‌هایی همانند هلی‌استون و ...)

•رهگیری و شناسایی هوشمند اطلاعات و داده‌های رایانه‌ای فضای سایبری از طریق شنود رایانه‌ها و نرم افزارهای جاسوسی[4].[20]

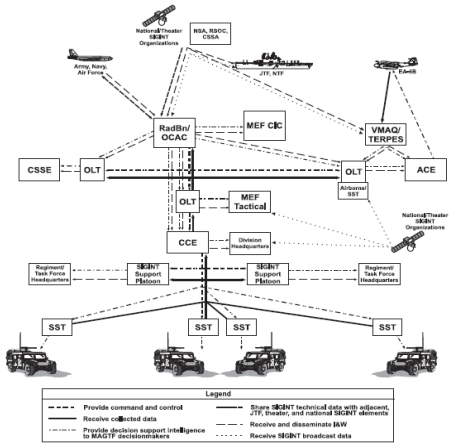
• جمع‌آوری هوشمند اطلاعات و داده‌های سایبری با استفاده نرم افزارهای جاسوسی در فضای سایبری.[21]

• همگرایی و یکپارچه‌سازی اطلاعات ارتباطی با جنگ سایبری و جنگ الکترونیک(سایبر الکترونیک).[22]

[1] - حساسه‌های اطلاعات ارتباطی پرفت(PRHEAT) زمین پایه

[2] - SHADW
[3] - PSS2

[4] - جاسوس‌افزار



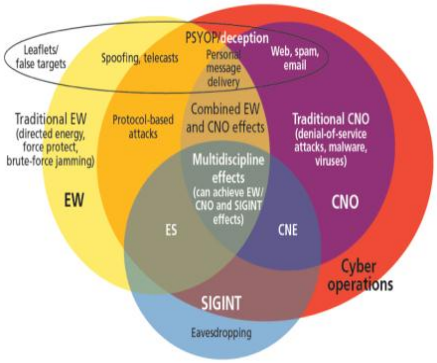
شکل ۲- معماری عملیات اطلاعات سیگنالی(اطلاعات ارتباطی) آمریکا[23]

پ- همگرایی عملیات سایبرالکترونیک آمریکا: در طیف الکترومغناطیس و فضای سایبری با روش‌های ابتکاری و پیچیده جهت پیشبرد اهداف و حمله الکترونیکی با استفاده ترکیبی از عملیات شبکه‌های رایانه‌ای و جنگ الکترونیک (سایبرالکترونیک) به منظور تأثیرگذاری بر فضای مجازی و طیف الکترومغناطیس به عنوان یک عملکرد راه‌کنشی و عملیاتی اقدام می‌نمایند.

تجزیه و تحلیل عملیات شبکه‌ای در اینترنت، فعالیت‌های ارتباطی بردبلند از قابلیت‌های سامانه‌های رایانه‌ای، پردازشگرها و کنترلرهای مربوطه با امکان حضور و بهره‌برداری از قابلیت‌های سازمان سایبری و جنگ الکترونیک.[24]

مهمترین طرح‌های آتی یکپارچگی و یکنواختی فضای سایبری و طیف الکترومغناطیسی (سایبرالکترونیک)؛ برنامه‌ریزی جهت تسلط بر تمامی طیف الکترومغناطیسی، تجمیع و کوچک‌سازی ساختار سازمانی اطلاعات سیگنالی و جنگ الکترونیک و بکارگیری سامانه‌های چند منظوره بجای سامانه‌های تک منظوره می‌باشد.[25]

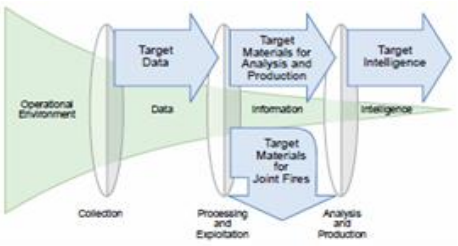
از اهداف و اولویت‌های اولیه فرماندهی سایبری ارتش آمریکا، ایجاد قابلیت سایبر الکترونیک برای تأثیرگذاری در فضای سایبری به منظور پشتیبانی از عملیات جنگ الکترونیک است که به صورت هماهنگ و هم‌زمان شده توسط سازمان رزم در منطقه عملیاتی اجرا می‌گردد. عملیات شبکه، جنگ شبکه، عملیات شبکه رایانه‌ای، برتری‌های فضائی و جنگ الکترونیک از جمله قابلیت‌های سایبر الکترونیک است که مورد توجه فرماندهان عملیات راه‌کنشی صحنه نبرد قراردارد. ایجاد یکپارچگی در مدیریت موضوعات سایبری، طیف الکترومغناطیس و اطلاعات باعث هم‌افزایی قابلیت‌های سازمان در اقدامات جنگ الکترونیک و عملیات شبکه خواهد شد. یگان‌هایی همچون فرماندهی امنیت و اطلاعات، فرماندهی شبکه[1] نیروهای مسلح و فرماندهی اعلام خطر و هشدار دهنده[2] در این فرآیند همکاری می‌نمایند.[26]



شکل ۳- فضای سایبر الکترونیک در ماموریت جدید سایبری امریکا

ت- سیکل تبدیل داده‌ها، به اطلاعات در سامانه‌های اطلاعات سیگنالی آمریکا

انجام عملیات نیازمند اطلاعات می‌باشد که از طریق سیکل اطلاعات در مراحل جمع‌آوری، پردازش، تجزیه و تحلیل، توزیع اطلاعات و بازخورد و ارزیابی اطلاعات می‌باشد. بنابراین سامانه‌های اطلاعات ارتباطی آمریکا مطابق الگوریتم زیر داده‌های جمع‌آوری شده را به اطلاعات قابل استفاده تبدیل می‌نماید.

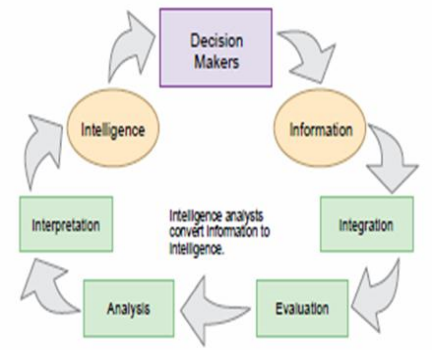


شکل٤- مراحل تبدیل داده و خبر به اطلاعات در سامانه‌های اطلاعاتی آمریکا. [27]

ث-تجزیه و تحلیل و تولید اطلاعات ارتباطی

به منظور تبدیل اخبار اطلاعات جمع‌آوری شده به اطلاعات قابل مصرف می‌بایست ابتدا یکپارچه‌سازی، ارزیابی، تجزیه و تحلیل و تفسیر نمود تا داده‌های جمع‌آوری شده به اطلاعات مورد نیاز برای عملیات استخراج شود، که این اطلاعات مبنایی برای تصمیم‌گیری برای انجام عملیات می‌باشد.

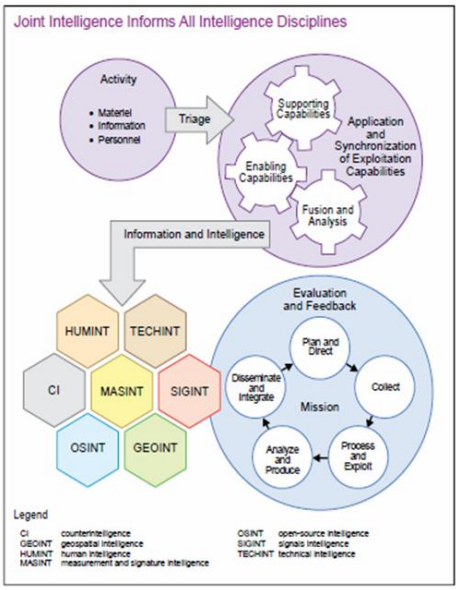
[1]-NETCOM
[2]-REDCOM



شکل۵- تحلیل و تولید اطلاعات جهت تصمیم‌گیری میران نبرد در اطلاعات ارتباطی آمریکا [28]

ج- ادغام اطلاعات

در عملات‌های مشترک نیاز هست همه گروه‌های اطلاعات شامل اصلاعات‌انسانی، اطلاعات فنی، اطلاعات سیگنالی، اطلاعات سنجشی و علائمی، اطلاعات جغرافیایی، اطلاعات منابع آزاد، اطلاعات تصویری به منظور انجام ماموریت نیاز می‌باشد. در صورت این مجموعه کامل است که در ادغام اطلاعات نقش همه گروه‌های اطلاعاتی لحاظ شود. مرکز عملیات مشترک آمریکا به لحاظ کردن الگوریتم فوق این نقش را ایفا می‌نماید.



شکل٦- انجام عملیات مشترک نیازمند ادغام در همه گروه‌های اطلاعاتی می‌باشد. [29]

چ- نقش فناوری در جمع‌آوری اطلاعات آمریکا از کشورهای مختلف.

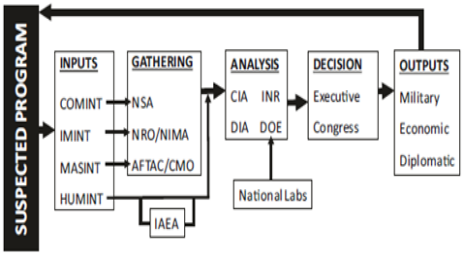
آمریکایی‌ها با استفاده از ماهواره‌ها، هواپیماهای با سرنشین و بدون سرنشین،حساسه‌های اطلاعات ارتباطی، حساسه‌های سنجشی و علائمی از کل دنیا با استفاده از برنامه‌های ویژه و خاص خود اطلاعات اطلاعات مورد نیاز خود را جمع‌آوری می‌نماید.

	Iraq-81	Iraq-91	Iraq-03	Syria	Iran	DPRK
Satellite	✓	✓	✓	✓	✓	✓
Spy planes	?	✓	✓	?	✓	✓
Drones					✓	✓
COMINT	✓	✓	✓	?	✓	✓
MASINT		✓		✓		✓
IAEA	✓	✓	✓	✓	✓	✓
Defectors		✓	✓		✓	✓

[30]

ح- برنامه‌های پشتیبانی اطلاعاتی امریکا

آژانس امنیت ملی آمریکا، مصرف کننده اصلی اطلاعات ارتباطی است که در کنار سایر گروه‌های اطلاعاتی، اطلاعات سامانه‌های ارتباطی و سایبری جمع‌آوری می‌نماید که خروجی این کار استخراج اطلاعات نظامی، اطلاعات اقتصادی و اطلاعات سیاسی می‌باشد و مبنایی برای تصمیم‌گیری و تصمیم‌سازی کلیه برنامه‌ها راه‌کنشی و راهبردی می‌باشد.



[31]

خ- کاربردهای سامانه‌های ارتباطی

شبکه‌های ارتباطی اصولا بسیار پیچیده و گسترده هستند. شبکه‌ها می‌بایستی از مرکز ستاد فرماندهی از طریق سطوح مختلف فرماندهی به واحدهای مختلف عملیاتی که ممکن است در فاصله دور یا نزدیک، در فضا یا روی زمین یا حتی زیرسطح دریا باشند، برسند که انواع شبکه‌های ارتباطی شامل؛ شبکه‌های ارتباطی ساده یک‌طرفه، شبکه ارتباطی دو طرفه، ارتباطات ترکیبی(مرکب)، شبکه ارسال دائم، سامانه ارتباطی مایکروویو(ارتباطات‌تروپسفری، تله‌متری، ارتباطات ماهواره‌ای) می‌باشند. شبکه‌های ارتباطات تلفنی شامل؛ تلفن و مراکز مخابراتی، تلفن بدون سیم، تلفن همراه، شبکه‌های ارتباطی در سامانه فرماندهی و کنترل، شبکه‌های چند کاناله ثابت برای استفاده راهبردی، شبکه‌های ثابتHF تک کاناله، شبکه چندکاناله متحرک با کاربردهای راهکنشی، شبکه‌های یک کاناله متحرک برای کاربردهای راهکنشی، شبکه‌های دارای اشتراک زمانی می‌باشند. [32]

روش‌های ارسال در این شبکه‌ها بصورت دور برد راهکنشی و گاهی اوقات راهبردی، ارسال زمینی راهکنشی، سامانه‌های تقویت رادیویی و ارتباطات زمین به هوا و هوا به هوای

راهکنشی، ارسال انتشارات تروپوسفری، ارسال ماهواره‌ای، ارسال فیبرنوری برای شبکه‌های محلی، ارسال با سکوهای زیر آب، انتشار در باند فرکانس بالا، ارسال در باند فرکانس خیلی بالا، ارسال‌ها با انفجار شهاب سنگی، ارسال در باندUHF، ارسال مایکرویو، ارتباط توسط پخش‌کننده تروپسفری، ارتباطات ماهواره‌ای، ارتباطات فیبر نوری، ارتباط با سکوهای در زیر آب، مخابرات شهاب سنگی، امواج میلی‌متری، مخابرات نوری، مخابرات نوترینو، شبکه‌های ناحیه محلی، مخابرات طیف گسترده می‌باشد.[33]

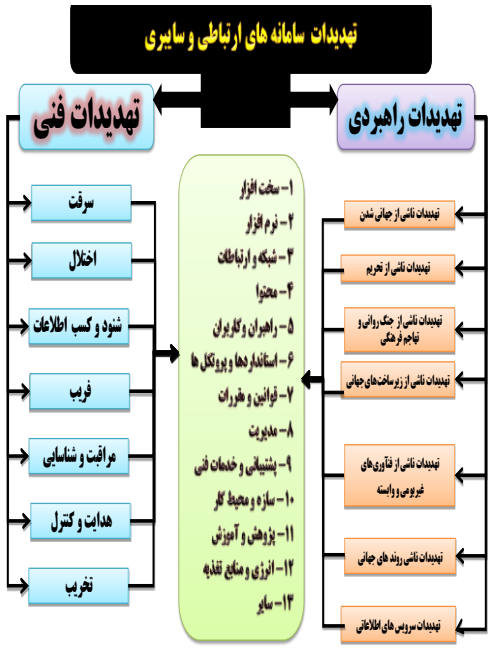
د- مؤلفه‌های اصلی پدافند غیرعامل ارتباطی

بر اساس نتایج حاصله از پرسش‌نامه در بین جامعه خبره، مؤلفه‌های اصلی پدافند غیرعامل ارتباطی با موافقت اکثریت(بیش از ۸۰٪) عبارتند از:"مولفه‌های اصلی پدافند غیرعامل ارتباطی؛ کاهش آسیب‌پذیری سامانه‌های ارتباطی، تداوم فعالیت‌های ضروری،بازدارندگی، ارتقاء پایداری ارتباطات ملی، تسهیل مدیریت بحران ارتباطی و مصون‌سازی حوزه ارتباطی کشور می‌باشد."

ذ- تهدیدهای مختلف سامانه‌های ارتباطی و سایبری:

حوزه‌های تهدیدات و اقدامات موثر بر علیه سامانه‌های ارتباطی و سایبری مورد استفاده در سامانه‌های فرماندهی و کنترل عبارتند از:

جدول۱.حوزه‌های تهدید بر علیه سامانه‌های ارتباطی و سایبری.



[34]

ر- اصول پدافند غیرعامل ارتباطی در برابرتهدیدهای حساسه‌های اطلاعات ارتباطی:

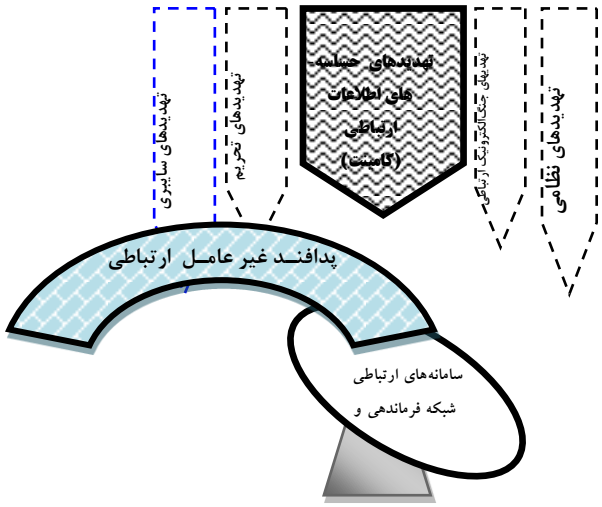
بر اساس نتایج حاصل از پرسش‌نامه توزیع‌شده بین خبرگان جامعه آماری، اصول پدافند غیرعامل ارتباطی عبارتند از:" اصل‌های فریب، توزیع و پراکندگی، پنهان‌کاری، استتار(درون شبکه‌ای و برون شبکه‌ای)، اختفاء و خفیفه‌نگاری، مصون‌سازی، رمزنگاری و خفیفه‌نگاری، استحکام و مقاوم سازی(دیواره آتش، کنترل دسترسی و سامانه‌های نرم‌افزاری)، کنترل انتشارات، کاهش آسیب‌پذیری، آمایش سرزمینی، چابکی و چالاکی(تحرک و جابجایی سریع)، احتمال رهگیری و آشکارسازی کم، فرماندهی و کنترل هوشمند، پشتیبانی الکترونیکی، حفاظت الکترونیکی و تسهیل مدیریت بحران در سامان‌های ارتباطی."

ز- اقدامات پدافند غیرعامل ارتباطی:

بر اساس مطالعه ادبیات تحقیق توسط محقق و نتایج حاصل از مصاحبه و پرسش‌نامه توزیع‌شده بین خبرگان جامعه آماری پژوهش عبارتند از؛

- کنترل تشعشعات سامانه‌های ارتباطی(مدیریت هوشمند طیف فرکانس ارتباطی).
- فریب الکترونیکی و غیرالکترونیکی بصورت نرم‌افزاری و سخت افزاری در سامانه‌های ارتباطی.
- استتار، اختفاء، بدل‌سازی، شبیه‌سازی، تحرک و جابجایی سریع، ارتباطات لایه به لایه و آنتن‌های جهتی و چندمنظوره سامانه‌های ارتباطی.
- رمزنگاری و پنهان‌نگاری نرم‌افزاری و سخت‌افزاری کلیه ارتباطات سامانه‌های ارتباطی.
- بکارگیری احتمال بسیار کم شنود در سامانه‌های ارتباطی(با استفاده از مخابرات نوری در اتباطات با هدف نرخ داده بالا، امنیت فوق العاده بالا.)
- بکارگیری فناوری طیف گسترده در ارتباطات با روش‌های پوششی(پرش فرکانس، ارسال سریع، رانش صفر، توالی مستقیم، یکنواختی شکل پیام، رمزنگاری)
- آمایش سامانه‌های ارتباطی به منظور کاهش و عدم رهگیری توسط حساسه‌های اطلاعات ارتباطی.

س- الگـــوی مفهومـــی تحقیق



۳- روش شناسی تحقیق

این پژوهش از نظر هدف کاربردی و با توجه به این که برای اولین بار انجام می‌شود، توسعه‌ای و روش تحقیق آمیخته از نوع موردی-زمینه‌ای می‌باشد. روش گردآوری اطلاعات بصورت کتابخانه‌ای با مطالعه اسناد و مدارک موجود و ابزار آن بررسی اسناد و مدارک، آرشیو، کتاب، استفاده از اطلاعات موجود در وبگاه اینترنت در زمینه اطلاعات ارتباطی، سایبری و ارتباطی، فرماندهی و کنترل و مصاحبه و با استفاده از پرسش‌نامه جهت اخذ نظر خبرگان استفاده شده است. به منظور تجزیه و تحلیل و ارایه راهبردها از روش نوین تدوین راهبرد دیوید استفاده شده و سپس با استفاده از روش خبرگی عوامل محیطی(قوت، ضعف، تهدیدها و فرصت‌ها) احصاء و با استفاده از ماتریسSWOT جهت تدوین راهبرد و استفاده از نرم‌افزار TOPSIS در تعیین اولویت راهبردهای و سپس اقدام به تجزیه و تحلیل اطلاعات شده است. قلمرو زمانی پژوهش مربوط به تهدیدهای از پنج سال قبل تاکنون خواهد بود و پیشنهاداتی برای افق ده سال آتی برای افق چشم‌انداز کشور۱٤۰٤تا پایداری عوامل محیطی دارد. قلمرو مکانی سامانه‌های ارتباطی شبکه فرماندهی و کنترل جمهوری اسلامی ایران می‌باشد. جامعه آماری ٦۰ نفر به صورت تمام شمار، شامل فرماندهان، صاحب‌نظران، خبرگان و نخبگان، متخصصان، کارشناسان و اساتید دانشگاه در حوزه‌های اطلاعات ارتباطی، سایبری، جنگ الکترونیک، سامانه‌های ارتباطی، پدافند غیرعامل و فرماندهی و کنترل که دارای حداقل ۱۵سال سابقه اجرایی و مدیریتی و حداقل دارای مدرک تحصیلی کارشناسی ارشد(٦٦٪ دکتری و ۳٤٪ کارشناسی ارشد) می‌باشد. روایی پرسش‌نامه به تایید خبرگان و اساتید دانشگاهی رسیده و پایایی آن با استفاده از آزمون آلفای کُرُنباخ ۰/۸۷ بوده که نشانگر پایایی پرسش‌نامه می‌باشد.

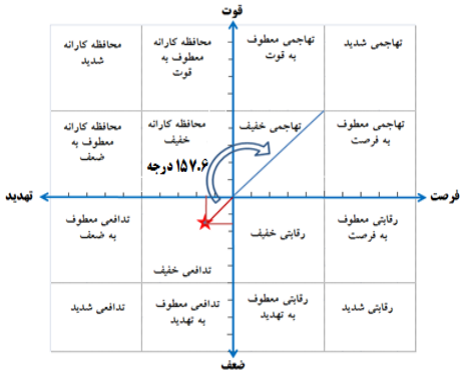
٤- تجزیه و تحلیل داده‌های تحقیق

الف- تجزیه وتحلیل داده‌ها

(۱)- ماتریس ارزیابی موقعیت و اقدام راهبردی[1]

جهت تعیین موقعیت راهبردی و تحلیل شکاف از ماتریس IFE & EFE بدین صورت عمل کرد:

مختصات وضع موجود= (A, B)	
نمره موزون ضعف‌ها - نمره موزون قوت‌ها = A	-0.68915
نمره موزون تهدیدات- نمره موزون فرصت‌ها = B	-1.65482
C = Arctg A/B	22.6°
D= زاویه نقطه مطلوب(ایده‌آل) با محور X ها	٤٥°
مقدار زاویه چرخش راهبردی از وضع موجود به سمت وضع مطلوب =C+D	
$22.6°+90°+45°=157.6°$	



مقدار زاویه چرخش از وضع موجود به وضع مطلوب برابر با ۱۵۷,٦°درجه می‌باشد. وضع موجود پدافند غیرعامل ارتباطی در ناحیه تدافعی یا انفعالی است و تا حدودی تهدید محور و در وضعیت ناپایداری است که در مواجهه با تهدیدهای آسیب‌پذیر می‌باشد و از نظر منابع و امکانات تخصصی با مشکل مواجه است و تاکید بر دستیابی به سامانه‌های نوین پدافند غیرعامل ارتباطی با رویکرد راه‌کارهای ناهمتراز و میانبر و خلاقانه مدنظر می‌باشد. بنابراین برای رسیدن به وضع مطلوب باید به رویکرد مقتدرانه آموزش، تحقیق، توسعه و تولید پدافند غیرعامل ارتباطی هوشمند و بومی در سامانه‌های ارتباطی با فناوری‌های نوین به رویکرد تهاجمی یا فعال برسیم، به فرصت‌ها توجه بیشتری از قوت‌ها و به نقاط ضعف و قوت داخلی توجه بیشتری شود. بنابراین پدافند غیرعامل ارتباطی به وضعیت پایدار و مطلوبی خواهد رسید.

(۲)- ماتریس ارزیابی عوامل داخلی(IFE):

[1]- Strategic Position And Action Evaluation Matrix (SPACE)

به منظور تحلیل محیطی پرسش‌نامه‌ای تهیه و در بین جامعه آماری توزیع و نتایج عبارتند از:

جدول ۲-فرصت‌های پدافند غیرعامل ارتباطی

شماره فرصت	نقاط فرصت
O1	استفاده از توان علمی دانشگاه‌های نظامی و غیرنظامی کشور در طراحی، ساخت سامانه‌های ارتباطی بومی در شبکه فرماندهی و کنترل.
O2	بکارگیری انواع فناوری‌های ضدشنود الکترونیکی در سامانه‌های ارتباطی.
O3	بکارگیری سامانه فرماندهی و کنترل هوشمند بومی.
O4	بکارگیری موثر شبکه‌های ارتباطی فیبرنوری در سامانه‌های ارتباطی و سایبری کشور.
O5	استفاده از سازه‌های دفنی ارتباطی با هدف پوشش و اختفاء سامانه‌های ارتباطی.
O6	بکارگیری اقدامات حفاظت الکترونیکی(پدافند غیرعامل ارتباطی) در سامانه‌های ارتباطی.
O7	بکارگیری انواع سامانه‌های فریب ارتباطی به صورت الکترونیکی و غیرالکترونیکی.
O8	بکارگیری فناوری طیف گسترده در سامانه‌های ارتباطی بومی.
O9	تحرک، جابجایی بسیار سریع سامانه‌های ارتباطی.
O10	بکارگیری رمزنگاری پیشرفته هوشمند بومی در سامانه‌های ارتباطی و سایبری کشور.
O11	بکارگیری فناوری خفیفه‌نگاری[1] بومی در سامانه‌های ارتباطی و سایبری
O12	استفاده از ارتباطات چندلایه در سامانه‌های فرماندهی و کنترل.

فرصت	تطابق با عامل		وضع موجود(اهمیت)	
	میانگین	وزن	میانگین (ضریب اهمیت)	نمره موزن (وزن عامل)
O1	۴،۹۹	0.0422344	۳،۲۴	0.13684
O2	۴،۱۷	0.0352941	۳،۲۶	0.032296
O3	۴،۴	0.0372408	۳،۷۸	0.037448
O4	۳،۹۸	0.033686	۲،۶۷	0.089942
O5	۳،۷۶	0.031824	۲،۲۳	0.070967
O6	۳،۷۸	0.0319932	۲،۹۸	0.09534
O7	۳،۳۴	0.0282691	۳،۱۶	0.089331
O8	۳،۸۷	0.032755	۳،۴۵	0.113005
O9	۳،۷۷	0.0319086	۲،۸۷	0.091578
O10	۴،۱۲	0.0348709	۲،۶۸	0.093454
O11	۳،۹۱	0.0330935	۲،۸۳	0.093655
O12	۴،۷۶	0.0402878	۲،۹۸	0.120058
جمع	48.85	0.413457	36.13	1.06391

جدول۳- تهدیدهای پدافند غیرعامل ارتباطی

شماره تهدید	تهدیدها
T1	توانایی ایجاد اختلال الکترونیکی بر روی سامانه‌های ارتباطی.
T2	توانایی ایجاد فریب الکترونیکی بر روی سامانه‌های ارتباطی.
T3	توانایی استفاده از پایگاه‌های نظامی آشکار و پنهان توسط آمریکا در همسایگی ایران.
T4	توانایی استفاده از سکوهای فضاپایه جمع‌آوری اطلاعات ارتباطی در رهگیری و شناسایی سامانه‌های ارتباطی.
T5	توانایی استفاده از سکوهای جمع‌آوری اطلاعات ارتباطی باسرنشین و بدون سرنشین هواپایه.
T6	توانایی حمله و اختلال سایبری بر روی فرستنده‌های ارتباطی.
T7	توانایی استفاده از سکوهای دریاپایه جمع‌آوری اطلاعات ارتباطی سطحی و زیرسطحی توسط آمریکا در منطقه.
T8	توانایی استفاده از فرماندهی اطلاعات و امنیت با بکارگیری مراکز عملیات امنیت منطقه‌ای، مرکز تجزیه و تحلیل اطلاعات ارتباطی، مرکز عملیات امنیت ملی در کنار سایر نیروهای مسلح آمریکا از زمین، دریا، هوا، فضاو فضای سایبری در رهگیری، موقعیت‌یابی، شناسائی، اختلال و انهدام سامانه‌های ارتباطی کشور.
T9	توانایی تشخیص آرایش نظامی الکترونیکی و آمایش سرزمینی سامانه‌های ارتباطی توسط حسامسه‌های اطلاعات ارتباطی.
T10	همگرایی و یکپارچگی جنگ سایبری و جنگ الکترونیک (سایبرالکترونیک) آمریکا با هدف تسلط بر سامانه‌های ارتباطی.
T11	توانمندی‌های عملیات اطلاعاتی آمریکا در محورهای؛ عملیات روانی، فریب نظامی، حفاظت اطلاعات، عملیات شبکه رایانه‌ای و جنگ‌الکترونیک (سایبر الکترونیک).
T12	توانایی رهگیری، شناسایی و رمزگشایی سامانه‌های ارتباطی توسط حسامسه‌های اطلاعات ارتباطی و سایبری.
T13	بکارگیری گسترده سامانه‌های جمع‌آوری اطلاعات ارتباطی و سایبری همانند شبکه جهانی جاسوسی اشلون، پریزم و سایر سازمان‌های اطلاعات ارتباطی.
T14	برخورداری از توانمندی‌های مرکز عملیات منطقه‌ای[2] آمریکا در پایگاه العدید قطر.

چون عدد تهدیدها بیش از عدد فرصت‌هاست، بدین معناست که سامانه‌های ارتباطی شبکه فرماندهی و کنترل کشور در برابر تهدیدهای حساسه‌های اطلاعات ارتباطی در محیط خارجی با تهدید روبرو است.

(۳)- ماتریس ارزیابی عوامل خارجی(EFE)

جدول٤- قوت‌های پدافند غیرعامل ارتباطی

قوت	نقاط قوت
S1	بهره‌برداری از الگوهای پدافند غیرعامل از منظر قرآن کریم، آموزه‌های دینی.
S2	تدابیر و سیاست‌های ابلاغی پدافند غیرعامل از سوی مقام معظم رهبری(مدظله العالی)
S3	وجود اسناد بالادستی در حوزه‌ی پدافند غیرعامل در قانون اساسی و برنامه‌های توسعه چهارم، پنجم و ششم کشور.
S4	توانایی آموزش‌های کلاسیک پدافند غیرعامل در سامانه‌های ارتباطی با استفاده از توان علمی دانشگاه-های نظامی و غیرنظامی.

تهدید	تطابق با عامل		وضع موجود(اهمیت)	
	میانگین	وزن	میانگین (ضریب اهمیت)	نمره موزن (وزن عامل)
T1	4.78	0.040457	4.12	0.166683
T2	4.56	0.038595	4.76	0.183712
T3	4.98	0.0421498	4.23	0.178294
T4	5.23	0.0442658	4.67	0.206721
T5	5.27	0.0446043	4.88	0.217669
T6	4.92	0.041642	4.12	0.171565
T7	4.24	0.0358866	4.98	0.178715
T8	5.82	0.0492594	4.89	0.240879
T9	4.68	0.0396107	4.17	0.165176
T10	4.99	0.0422344	4.99	0.21075
T11	4.63	0.0391875	4.43	0.173601
T12	5.34	0.0451968	4.87	0.220108
T13	4.99	0.0422344	4.96	0.209483
T14	4.87	0.0412188	4.74	0.195377
جمع	69.3	0.5865425	64.81	2.718733
جمع‌کل	118.15	۱	100.94	3.782645

[1] -STEANOGRAPHY

[2] - CENTCOM

S5	طراحی، ساخت و بکارگیری سامانه‌های ارتباطی مجهز به فناوری‌های پدافند غیرعامل ارتباطی بومی .
S6	طرح‌ریزی، اجرا و آمایش سرزمینی سامانه‌های ارتباطی در سطوح عملیاتی، تاکتیکی و راهبردی.
S7	وجود سامانه‌ی فرماندهی و کنترل هوشمند بومی.
S8	خوداتکایی حداکثری در شبکه‌های ارتباطی سامانه‌های فرماندهی و کنترل از سایر شبکه‌های ارتباطی کشور.
S9	برخورداری از شبکه گسترده فیبرنوری در کشور.
S10	بکارگیری عملیات رمز های پیشرفته در کلیه سطوح ارتباطی شبکه فرماندهی و کنترل.
S11	استفاده از شبکه‌های ارتباطی لایه به لایه‌ی بومی.
S12	برخورداری از شبکه‌های ارتباطی پشتیبان و جایگزین در شرایط اضطراری و بحران.
S13	رعایت حداکثری اقدامات و الزامات پدافند غیرعامل ارتباطی بومی در برابر حساسه‌های اطلاعات ارتباطی.
S14	توانایی مقابله با اختلات الکترونیکی و سایبری در سامانه‌های ارتباطی.

قوت	تطابق با عامل		وضع موجود(اهمیت)	
	میانگین	وزن	میانگین (ضریب اهمیت)	نمره موزن (وزن عامل)
S1	4.23	0.032009	3.12	0.09986833
S2	4.23	0.032009	4.31	0.13795914
S3	4.45	0.033674	4.21	0.14176693
S4	4.22	0.031933	4.26	0.13603632
S5	4.23	0.032009	4.12	0.13187741
S6	4.24	0.032085	4.36	0.13988952
S7	4.16	0.031479	4.41	0.13882406
S8	4.59	0.034733	4.13	0.14344835
S9	4.41	0.033371	4.12	0.13748922
S10	4.23	0.032009	4.51	0.14436095
S11	4.29	0.032463	4.23	0.13731896
S12	4.19	0.031706	4.12	0.13063034
S13	4.33	0.032766	4.11	0.13466742
S14	4.12	0.031177	4.09	0.12751267
جمع	59.92	0.453424	58.1	1.88164964

جدول۵- ضعف‌های پدافند غیرعامل ارتباطی

ضعف	نقاط ضعف
W1	به روز نبودن بعضی از سامانه‌های ارتباطی شبکه فرماندهی و کنترل کشور.
W2	نهادینه نشدن آموزش‌های پدافند غیرعامل ارتباطی.
W3	کافی نبودن فناوری‌های حفاظت الکترونیکی در سامانه‌های ارتباطی کشور.
W4	کافی نبودن الزامات پدافند غیرعامل‌ارتباطی در تامین، خرید و بکارگیری سامانه‌های ارتباطی.
W5	بومی نبودن برخی از سامانه‌های نرم‌افزاری و سخت افزاری مورد استفاده در سامانه‌های ارتباطی شبکه فرماندهی و کنترل.
W6	عدم بکارگیری سامانه‌های ارتباطی هواپایه (باسرنشین و بدون‌سرنشین) به منظور افزایش قدرت تحرک و جابجایی بسیار بالا.
W7	عدم گستردگی کامل و وسیع شبکه فیبرنوری در ارتباطات با نرخ داده و امنیت بسیار فوق‌العاده.
W8	کافی نبودن فناوری‌های پدافند غیرعامل ارتباطی با هدف مصون‌سازی در برابر حساسه‌های اطلاعات ارتباطی آمریکا.
W9	عدم استقاده وسیع از فناوری طیف گسترده در سامانه‌های ارتباطی شبکه فرماندی و کنترل.
W10	بومی نبون برخی از سامانه‌های نرم‌افزاری و سخت‌افزاری در سامانه‌های ارتباطی.
W11	کافی نبودن استفاده از دانش و فناوری‌های نوین و پیشرفته پدافند غیرعامل ارتباطی.
W12	امکان ایجاد فناوری‌های اختلال الکترونیکی بر روی سامانه‌های ارتباطی و سایبری.
W13	امکان ایجاد فریب الکترونیکی بر روی سامانه‌های ارتباطی.
W14	امکان شناسایی آمایش سامانه‌های ارتباطی توسط حساسه‌های اطلاعات ارتباطی.
W15	قابلیت رهگیری، شناسایی، رمزگشایی و موقعیت‌یابی سامانه‌های ارتباطی توسط حساسه‌های اطلاعات ارتباطی.
W16	قابلیت رهگیری، شناسایی و ایجاد اختلال در سامانه‌های سایبری مورد استفاده در شبکه فرماندهی و کنترل.

چون عدد ضعف‌ها بیش از عدد قوت‌هاست، بنابراین پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل کشور در محیط داخلی با ضعف روبرو است.

ب- تجزیه وتحلیل سایرداده‌ها ویافته‌های تحقیق:

ضروری است با تخصیص منابع به نقطه مطلوب برسیم، بنابراین

ضعف	تطابق با عامل		وضع موجود(اهمیت)	
	میانگین	وزن	میانگین (ضریب اهمیت)	نمره موزن (وزن عامل)
W1	4.32	0.03269	4.75	0.15527809
W2	3.89	0.029436	5.96	0.17544003
W3	4.03	0.030496	4.12	0.12564207
W4	4.98	0.037684	4.75	0.17900114
W5	4.28	0.032387	4.98	0.16128944
W6	4.99	0.03776	4.38	0.16538933
W7	4.84	0.036625	4.85	0.17763148
W8	4.78	0.036171	4.77	0.17253575
W9	4.98	0.037684	4.93	0.18578434
W10	3.96	0.029966	4.28	0.12825426
W11	4.29	0.032463	4.33	0.14056527
W12	4.73	0.035793	4.65	0.16643587
W13	4.87	0.036852	4.87	0.17946954
W14	4.39	0.03322	4.73	0.15712978
W15	3.97	0.030042	4.38	0.13158229
W16	4.93	0.037306	4.54	0.16936966
جمع	72.23	0.546576	75.27	2.57079834
جمع‌کل	132.15	1	133.37	4.45244798

تقسیم‌بندی و تخصیص منابع عبارتند از:

جدول ٦- تقسیم‌بندی و تخصیص منابع

عوامل/ درصد منابع تخصیص یافته	مقادیر
قــوت	1.88164964
ضعف	2.57079834
فــرصت	1.06391
تهــدید	2.718733
مجموع قوت و ضعف	4.45244798
مجموع فرصت و تهدید	3.782645
زاویه بین دو پاره‌خط(درجه)	١٥٧/٦
درصد منابع موردنیاز قوت و ضعف	54/06
درصد منابع موردنیاز فرصت و تهدید	45/94
درصد منابع موردنیاز جهت ارتقای قوت	22/85
درصد منابع موردنیاز جهت رفع ضعف	31/21
درصد منابع موردنیاز جهت به‌کارگیری فرصت	12/92
درصد منابع موردنیاز جهت دفع تهدید	33/02

٥- نتیجه‌گیری

با اولویت‌بندی و تعیین مطلوبیت‌های راهبردی با استفاده از نظر ١٥ نفر خبره و نرم‌افزارTOPSIS، یافته‌های تحقیق به عنوان مناسب‌ترین راهبردهای پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل در برابر تهدیدهای شنود الکترونیکی توسط حساسه‌های اطلاعات ارتباطی دشمن عبارتند از:

١. استتار الکترونیکی سامانه‌های ارتباطی با استفاده از بکارگیری فناوری طیف گسترده با هدف کاهش و عدم رهگیری و شناسایی توسط حساسه‌های اطلاعات ارتباطی دشمن.

٢. پنهان‌کاری و پنهان‌نگاری سیگنال‌های ارتباطی و سایبری با هدف کاهش رهگیری و شناسایی توسط حساسه‌های اطلاعات ارتباطی از طریق بکارگیری فناوری‌های رمزنگاری و پنهان‌نگاری پیشرفته بومی در سامانه‌های ارتباطی و سایبری.

٣. مصون‌سازی سامانه‌های ارتباطی شبکه فرماندهی و کنترل از طریق بکارگیری الزامات و اقدامات پدافند غیرعامل ارتباطی بومی با هدف ارتقاء پایداری ملی.

٤. هوشمندسازی فناوری‌های حفاظت الکترونیکی ارتباطی از طریق بکارگیری هوش مصنوعی با هدف ارتقاء قابلیت انعطاف پذیری سامانه‌های ارتباطی در برابر تهدیدات.

٥. ایمن‌سازی سامانه‌های ارتباطی با هدف محروم‌سازی دشمن از طریق عدم دستیابی به اطلاعات و فناوری‌های ارتباطی از طریق رعایت امنیت اطلاعات و عدم افشای فناوری‌های پدافند غیرعامل ارتباطی بومی.

٦. چندمنظوره سازی سامانه‌های ارتباطی با هدف فریب حساسه‌های اطلاعات ارتباطی از طریق بکارگیری دام‌های فعال و غیرفعال.

٧. خودکفایی و خوداتکایی نرم‌افزاری‌و سخت‌افزاری سامانه‌های ارتباطی با هدف بومی سازی از طریق دانشگاه‌ها، مراکز تحقیقاتی و صنعتی.

٨. بومی‌سازی دانش پدافند غیرعامل ارتباطی با استفاده از توان علمی دانشگاه‌های نظامی و غیرنظامی کشور با هدف خودکفایی علمی کشور.

٩. پایش مستمر تهدیدهای برعلیه سامانه‌های ارتباطی و سایبری با هدف هشداردهی از طریق بکارگیری حساسه‌های مختلف جمع‌آوری اطلاعات.

١٠.آمایش سامانه‌های ارتباطی با هدف فریب و کاهش آسیب‌پذیری از طریق باز طراحی مجدد آمایش سامانه‌های ارتباطی در برابر تهدیدهای رهگیری و شناسایی حساسه‌های اطلاعات ارتباطی دشمن.

١١.پاسخگویی در برابر تهدیدها با هدف ارتقاء آمادگی رزمی از طریق اجرای رزمایشهای تخصصی پدافندغیرعامل ارتباطی.

١٢.فرهنگ‌سازی پدافند غیرعامل ارتباطی با استفاده از آموزش علمی در کلیه سطح با هدف نهادینه‌سازی در کشور.

٦ – نوآوری در تحقیق

نوآوری‌های این تحقیق عبارتند از:

الف- تدوین راهبردهای پدافند غیرعامل سامانه‌های ارتباطی شبکه فرماندهی و کنترل در برابرتهدیدهای شنود الکترونیکی توسط حساسه‌های اطلاعات ارتباطی دشمن.

ب- تدوین ادبیات پدافند غیرعامل ارتباطی می‌باشد.

پ- تدوین نقاط قوت و ضعف سامانه‌های ارتباطی و سایبری شبکه فرماندهی و کنترل.

ت- تدوین فرصت‌ها و تهدیدهای حساسه‌های اطلاعات ارتباطی.

۷-مراجع

[1]رزمخواه، محمدرضا.اسفندیاری، مسعود. سپهری،محمد .(۱۳۸۷). بررسی تطبیقی و پایش تهدیدات فناوری‌های جنگ الکترونیک هوایی و ترازیابی توان فناوری‌های جنگ الکترونیک هوایی دو کشور ایران و آمریکا و ارایه‌ی الگوی تحلیلی مناسب و استخراج فناوری‌ها و تجهیزات جنگ الکترونیک هوایی ایران و مستندسازی آن‌ها، تهران: موسسه‌آموزشی‌و تحقیقاتی صنایع دفاعی.صص ۶۲-۲۷۵

[2] عرفانی، اسماعیل. حسینی، سید احمد. سعیدآوی، جبار.(۱۳۹۲). جمع آوری، تجزیه و تحلیل و پردازش اطلاعات سامانه‌های جنگ الکترونیک ارتش آمریکا مستقر در خلیج فارس.تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی.صص ۲۴۰-۲۷۵

[3] لونی، محمدرضا.(۱۳۹۱).تدوین راهبرد ملی پدافند غیرعامل در حوزه ارتباطات،تهران: دانشگاه عالی دفاع ملی صص ۱۵-۳۶.

[4] سپهری، محمد.(۱۳۹۶). راهبردهای پدافند غیرعامل سامانه‌های راداری و ارتباطی آجا در مقابله با تهدیدات ناهمتراز از ناحیه حساسه‌های اطلاعات سیگنالی دشمن(رساله دکتری). تهران. دانشگاه عالی دفاع ملی.صص ۲۶۰-۲۶۸.

[5] موسوی،سیدعبدالرحیم.سپهری،محمد.دهقان،نبی‌الله.
نجاتی،منصور.(۱۳۸۸).راهبردهای پدافند غیرعامل الکترونیک آجا در برابر تهدیدات ناهمتراز حساسه‌های اطلاعات سیگنالی دشمن.فصل نامه مطالعات استراتژیک.

[6]محمدی،علی.موحدی‌صفت،محمدرضا.(۱۳۸۷).امنیت فضای تبادی اطلاعات کشور، پیش‌نیاز و حافظ اقتدار ملی.تهران: فصل‌نامه مطالعات دفاعی استراتژیکی دانشگاه عالی دفاع ملی.صص ۱۷.

[7] جلالی فراهانی، غلامرضا.(۱۳۹۱) مقدمه‌ای بر مبانی نظری پدافند غیرعامل با رویکرد تهدیدهای جدید. تهران: دانشگاه امام حسین(ع) صص ۱۳۳.

[8] واحدی، مرتضی.قیاسی، علی‌اکبر.(۱۳۹۰).کلیات جنگ الکترونیک.تهران: انتشارات حفاظت اطلاعات کشور،صص ۵۲.

[9] CLARK,MROBERT.(2004)..INTELLIGENCE ANALYSIS: A TARGET CENTRIC APPROACH. .PP153 .

[10] حسنی‌اژدری، سید مجید.(۱۳۹۲).پدافندغیرعامل ارتباطی.نوشهر:انتشارات دانشگاه علوم دریایی امام خمینی(ره).صص ۲۱.

[11] همان صص۲۲.

[۱۲]دیوید اس.آلبرتز- ریچارد ای.هایس.(۱۳۹۶). قدرت در لبه فرماندهی و کنترل در عصر اطلاعات، تهران،موسسه آموزشی و تحقیقاتی صنایع دفاعی، صص۱۶.

[13]. (www.khamenei.ir۹۱/۸/۷)

[14](www.khamenei.ir۱۳۹٤/٤/۱۵)

[15] جلالی فراهانی، غلامرضا. هاشمی فشارکی، سیدجواد.(۱۳۸۹). پدافند غیر عامل در آیینه قوانین و مقررات. تهران: سازمان پدافند غیر عامل.صص ۱۰.

[16] سازمان پدافند غیرعامل کشور.(۱۳۹۵). سند راهبردی پدافند غیرعامل الکترونیک کشور.تهران. صص۵.

[17] ایزدی، پیروز.(۱۳۹۳).اطلاعات نظامی. تهران:دافوس سپاه .صص ۲۳.

[18] (Campbell,2013: 12)

[19] اسفندیاری، مسعود. سپهری، محمد.(۱۳۸۷). بررسی تطبیقی و پایش تهدیدات فناوری‌های اطلاعات هوایی و ترازیابی توان فناوری‌های اطلاعات هوایی دو کشور ایران و آمریکا و ارایه‌ی الگوی تحلیلی مناسب و استخراج فناوری‌ها و تجهیزات اطلاعات هوایی ایران و مستندسازی آنها، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی ، صص ۱۲۳-۱۴۵.

[20] ابراهیم‌نژاد شلمانی، محمدابراهیم.(۱۳۸۹). مقدمه‌ای بر جنگ سایبر و تروریسم سایبر جلد اول.تهران: بوستان حمید.صص ۳۴.

[21] کافی، سعید. (۱۳۹۳). تدوین راهبردهای پدافند غیرعامل در فضای سایبری زیرساخت‌های‌حیاتی ج.ا.ایران. (دکتری). دانشگاه عالی دفاع ملی، ایران.صص۱۱۲-۱۲۳.

[22](عرفانی و همکاران، ۱۳۹۲: ۸۵-۲۴۳)

[23]US Marine Corps.(2016).,Change all instances of MCWP 2-22, Signals Intelligence, to MCRP 2-10A.1. P47

[24](عرفانی و همکاران،(۲۳ :۱۳۹۲

[25] U.S. HOUSE of REPRESENTATIVES, 2008:8)

[26](همان،۲۵)

[27] Joint and National IntelligenceJoint and National Intelligence–5 July 2017 p 178

[28]۱۹۱ Joint and National IntelligenceJoint and National Intelligence–5 July 2017.p ۱۱۵

[29]۱۹۱Joint and National IntelligenceJoint and National Intelligence–5 July 2017 . p 143

[30]Technology and the Intelligence Community Challenges and Advances for the 21st Century-Margaret E. Kosal Editor-Margaret E. Kosal Georgia Institute of Technology Atlanta, Georgia, USA-2018 . p139

[31] Technology and the Intelligence Community Challenges and Advances for the 21st Century-Margaret E. Kosal Editor-Margaret E. Kosal Georgia Institute of Technology Atlanta, Georgia, USA-2018 .p 143

[32]سائسی، سیدمحسن، غفاری،مهبد.(۱۳۹۰).کاربرد سیستم های دفاع الکترونیکی ج۱. تهران: انتشارات نهاجا.ص ۲۷۱-۲۸۹.

[33] (نایبی و همکار:۱۳۹٤،۳۰٦-۲۹۱)

[34] پورابراهیم، علیرضا- پدافند ملی سایبری.(۱۳۹۲).- دانشگاه عالی دفاع ملی.ص۱۶.