ISSN:2821-1588 htpps://www.jadm.khadu.ir

فصلنامه علمی ((مدیریت دفاع هوایی))

سال اول ، شماره ۱ ، شهریور۱۴۰۱

مقاله پژوهشی

مناسب‌ترین راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در برابر تهدیدات آتی در افق چشم‌انداز ۱۴۰۴

محمد سپهری

۱- استادیار دانشگاه پدافند هوایی خاتم‌الانبیاء (ص)، تهران، ایران، (نویسنده مسئول)

اطلاعات مقاله

تاریخ پذیرش: ۱۴۰۰/۱۱/۰۳

تاریخ دریافت: ۱۴۰۰/۰۹/۲۲

کلمات کلیدی:

بحران، بحران‌های اجتماعی، فرماندهی و کنترل، مدیریت بحران‌های اجتماعی.

چکیده

جنگ‌های امروزی و آتی بر مبنای فناوری‌های جنگ الکترونیک طرح‌ریزی و اجرا می‌گردد. دفاع همه¬جانبه از کشور مستلزم شناخت دقیق و کافی از توانمندی¬های و فناوری‌های جنگ الکترونیک دشمن در تمامی حوزه¬های راداری و ارتباطی جهت مقابله با آنان می‌باشد. هدف اصلی مقاله دستیابی به مناسبت‌ترین راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در افق چشم‌انداز ۱۴۰۴ می‌باشد. در این مقاله پس از ارائه مطالبی مربوط به شناخت تهدیدها و توانمندی¬های جنگ الکترونیک دشمن، راه‌کارهای لازم جهت مقابله با تهدیدهای آنان به بررسی عملکرد نپاجا در استفاده از فناوری‌های جنگ الکترونیک می‌پردازد. این پژوهش کاربردی و توسعه‌ای، روش تحقیق آن آمیخته از نوع موردی‌زمینه‌ای، روش گردآوری اطلاعات اسنادی و پیمایشی و ابزار آن مصاحبه و جامعه آماری ۴۰ نفر می‌باشد که با استفاده از ماتریس SWOT جهت تجزیه‌وتحلیل محیط داخل و خارج و تدوین راهبردها و از نرم‌افزار TOPSIS در تعیین اولویت‌بندی راهبردهای جنگ الکترونیک نپاجا در مقابله با تهدیدهای دشمن استفاده گردید.

نویسنده مسئول:

محد سپهری

ایمیل:

sepehri377@chmail.ir

استناد به مقاله: محد سپهری (۱۴۰۰). مناسب‌ترین راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در برابر تهدیدات آتی در افق چشم‌انداز ۱۴۰۴ .فصلنامه علمی ((مدیریت دفاع هوایی)) سال اول ، شماره ۱ ، شهریور۱۴۰۰.

ISSN:2821-1588 htpps://www.jadm.khadu.ir

Journal of Air Defense Manegment

Research Paper

The most appropriate strategies for managing the battle scene of Air Defense Electronic warfare against future threats on the horizon of Vision 1404

Mohammad Sepehri

1- Assistant Professor, Khatam Ol Anbia (PBU) University, Tehran, Iran

Article Information

Accepted: 1400/11/03

Recceived:1400/09/22

Keywords:

Electronic warfare,
Electronic defense,
Electronic support,
Electronic attack,
Electronic protection.

Corresponding anuthor:
Mohammad Sepehri
Email:
sepehri377@chmail.ir

Abstract

Current and future wars are designed and implemented based on electronic warfare technologies. Comprehensive defense of the country requires accurate and sufficient knowledge of the capabilities and technologies of the enemy's electronic warfare in all areas of radar and communications to deal with them. The main purpose of this article is to achieve the most appropriate duration of the battle scene of Air Defense Electronic Warfare on the horizon of 1404. In this article, after presenting the issues related to recognizing the threats and capabilities of the enemy's electronic warfare, the necessary solutions to deal with their threats will examine the performance of Air Defense in the use of electronic warfare technologies. This applied and developmental research, its research method is mixed from case-context type, documentary data collection and survey method and its tools are interviews and statistical population of 40 people, which uses SWOT matrix to analyze indoor and outdoor environment and formulate strategies and TOPSIS software was used to determine the priority of Air Defense electronic warfare strategies in the face of enemy threats.

HOW TO CITE: Mohammad Sepehri (1400). The most appropriate strategies for managing the battle scene of Air Defense Electronic warfare against future threats on the horizon of Vision 1404. Journal of Air Defense Manegment.

۱. مقدمه

پیشرفت و توسعه صنایع الکترونیک، مخابرات و سایبر در تمامی حوزه‌های مختلف طیف الکترومغناطیس، باعث پیشرفت این علوم در حوزه نظامی گردید. اولین جهش الکترونیک به زمان استفاده از فرکانس‌های رادیویی برمی‌گردد که موجب ساخت و پیدایش رادار و سبب به وجود آمدن سامانه‌های دفاعی با سلاح‌های هدایت‌شونده گردید. تحول بعدی در سامانه‌های دفاعی، خصوصاً پدافندی باعث افزایش دقت هدایت موشک‌ها با خطای بسیار پایین که قادر به کشف دقیق محل اهداف و انهدام آن بوده، که برای کاهش و نابودی توان سامانه‌های دفاعی بکار می‌رفت. بنابراین سلاح‌های دقیق و پیشرفته کارایی خود را از دست دادند و هر کشوری که دارای سامانه‌های پیشرفته‌تر حمله الکترونیکی بود، پیروز میدان شد. اما پیشرفت‌ها به اینجا منتهی نگردید و ساخت و گسترش سامانه‌های حفاظت الکترونیک توسعه یافت تا توان و قابلیت سامانه‌های دفاعی در محیط جنگ الکترونیک همچنان پایدار بماند. بنابراین، هر فناوری که باعث ساخت وسایل الکترونیکی با توانایی کاهش کارایی سامانه‌های دفاعی دشمن شود، در جنگ الکترونیک حائز اهمیت می‌باشد و هرگونه تکنیک و فناوری که برای حذف یا کاهش اثرات مخرب سامانه‌های جنگ الکترونیک دشمن بکار می‌رود، در حفاظت الکترونیکی مدنظر می‌باشد. جنگ‌های امروزی به‌خصوص جنگ‌هایی که بعد از سال ۲۰۰۰ در منطقه خاورمیانه توسط نیروهای فرا منطقه‌ای، اتفاق افتاد، اکثراً بر اساس جنگ الکترونیک[1] طرح‌ریزی و اجرا گردید. در این تحقیق منظور از دشمن آمریکا و تهدیدات جنگ الکترونیک آن می‌باشد.

۱-۱ بیان مسئله

جنگ‌های امروزی در قرن بیست و یکم بر مبنای فناوری‌های مختلف جنگ اطلاعاتی، سایبری، شبکه محور و جنگ الکترونیک طرح‌ریزی و اجرا که باعث تخریب و عدم کارایی زیرساخت‌های حیاتی، حساس و مهم کشور هدف می‌گردد و جنگ الکترونیک می‌تواند جایگزین جنگ‌های سخت و فیزیکی گذشته شود و سبب فلج سازی راهبردی در بهره‌برداری از طیف الکترومغناطیس گردد. رویکرد جدید دشمن در سازمان‌دهی و ایجاد فرماندهی سایبری در رأس سازمان‌های جنگ الکترونیک و انتصاب سازمان و رده‌های جنگ‌های شبکه محور، جنگ اطلاعات به‌عنوان یگان‌های تحت امر این فرماندهی بیانگر این واقعیت است که امروزه هدف اصلی در جنگ حمله به تسلیحات و تجهیزات هوایی، زمینی و دریایی نیست بلکه حمله به شبکه‌ی اعصاب که همان شبکه اطلاعات و کلید زیرساخت‌های حیاتی یک کشور در طیف الکترومغناطیس می‌باشد. چون دشمن از سامانه‌های جنگ الکترونیک برای افزایش توانمندی و قابلیت‌های خود در میدان نبرد امروزی و آتی خود استفاده می‌نماید لازم است که این سامانه‌ها و قابلیت‌ها و توانمندی‌های آنان برای ما شناخته شده تا امکان مقابله بهتر و مناسب‌تر در برابر

[1] ELECTRONIC WARFARE

آنان فراهم گردد. بنابراین مسئله‌ی اصلی ما در این تحقیق مدون نبودن راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در برابر تهدیدهای آتی در افق چشم‌انداز ۱۴۰۴ دشمن می‌باشد.

۱-۲ اهمیت و ضرورت تحقیق

جنگ‌های امروزی و آتی به‌خصوص جنگ‌های نسل چهارم بر مبنای فناوری‌های مختلف جنگ الکترونیک در بخش‌های مختلف پشتیبانی الکترونیکی[1]، حمله الکترونیکی[2] و حفاظت الکترونیکی[3] طرح‌ریزی و اجرا می‌گردد. بر اساس همین اهمیت و حساسیت می‌باشد که مقام معظم فرماندهی کل قوا در دانشگاه هوایی شهید ستاری در مورخه ۱۰/۴/ ۱۳۸۱ و در دیدار با نیروی دریایی تأکید بسیار زیادی بر روی مسئله جنگ الکترونیک نمودند و فرمودند:"برای بالا بردن قابلیت‌های جنگ الکترونیک و مضاعف کردن آن در نیروها اهتمام بورزید. دنیا، دنیای جنگ الکترونیک است. همچنین در مراسم افتتاحیه ناوشکن جماران در مورخه ۸۹/۱۱/۳۰ فرمودند: من بارها در طی سال‌ها در دیدار با نیروی دریایی، هم در دیدار با نیروی هوائی، روی مسئله جنگ الکترونیک تأکید کرده‌ام، بازهم تأکید می‌کنم. (WWW.KHAMENEI.IR - ۸۹/۱۱/۳۰) فرمایشات معظم له اهمیت پرداختن به مسئله جنگ الکترونیک به‌عنوان راهبردی جهت مقابله با تهدیدات حملات الکترونیکی را مضاعف می‌نماید.

۱-۲-۱ اهمیت تحقیق

۱. شناسایی ساختار کلی سامانه‌های جنگ الکترونیک دشمن در سطوح عملیاتی، راه کنشی و راهبردی.
۲. شناخت توانمندی‌های سامانه‌های جنگ الکترونیک دشمن در منطقه.
۳. شناخت توانمندی‌ها و نقاط ضعف جنگ الکترونیک نپاجا در حوزه‌های مختلف در برابر حملات الکترونیکی دشمن.
۴. ایجاد بستری مناسب جهت ارتقاء توانمندی‌های جنگ الکترونیک نپاجا در بخش‌های پشتیبانی الکترونیکی، حمله الکترونیکی و حفاظت الکترونیکی.
۵. افزایش بازدارندگی، کاهش آسیب‌پذیری و مصون‌سازی در طیف الکترومغناطیس.

۱-۲-۲ ضرورت تحقیق

۱. عدم شناخت کافی تهدیدات جنگ الکترونیک منجر به غافلگیری راهبردی و فناوری در برابر حملات الکترونیکی دشمن می‌شود.
۲. در صورت نپرداختن به جنگ الکترونیک منجر به کشف و شناسایی بسیار آسان کلیه فعالیت‌های راداری و ارتباطی توسط حساسه‌های پشتیبانی الکترونیکی دشمن می‌گردد.
۳. در صورت عدم بررسی اقدامات و توانمندی‌های جنگ الکترونیک دشمن موجب بالا رفتن هزینه‌های

[1] ELECTRONIC SOPPORT(ES)
[2] ELECTRONIC ATTACK (EA)
[3] ELECTRONIC SUPPORT(ES)

دفاعی ما می‌گردد.

۴. در صورت نپرداختن به تجزیه‌وتحلیل تهدیدات جنگ الکترونیک دشمن منجر به ضربه خوردن از نقاط آسیب‌پذیر و فلج سازی راهبردی در طیف الکترومغناطیس خودی می‌گردیم.

۱-۳. هدف تحقیق

تدوین مناسب‌ترین راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در افق چشم‌انداز ۱۴۰۴.

۱-۳-۱ اهداف فرعی

۱. شناسایی تهدیدها و توانمندی‌های جنگ الکترونیک دشمن.
۲. شناسایی نقاط قوت و ضعف سامانه‌های جنگ الکترونیک نپاجا.

۱-۴. سؤال اصلی تحقیق

مناسب‌ترین راهبردهای مدیریت صحنه نبرد جنگ الکترونیک نپاجا در افق چشم‌انداز ۱۴۰۴ کدام‌اند؟

۱-۴-۱ سؤالات فرعی تحقیق

۱. تهدیدها و توانمندی‌های جنگ الکترونیک دشمن کدام‌اند؟
۲. نقاط قوت و ضعف سامانه‌های جنگ الکترونیک نپاجا کدام‌اند؟

۲. مبانی نظری و پیشینه پژوهش

۲-۱ مبانی نظری

انهدام دفاع هوایی دشمن[1]

فعالیتی است که با ابزارها و روش‌های تخریبی و یا مختل‌کننده در سامانه دفاع هوایی زمین پایه باعث خنثی‌سازی، انهدام یا کاهش موقت در قابلیت‌های دفاعی آن‌ها می‌شود [۱].

مدیریت طیف الکترومغناطیس

برنامه‌ریزی، هماهنگی و مدیریت استفاده مشترک از طیف الکترومغناطیس توسط روش‌های عملیاتی، مهندسی و اداری است که منظور از آن اعطای مجوز فعالیت به سامانه‌های الکترونیکی در محیط تهدید، بدون ایجاد هرگونه اختلال غیرقابل توجه است [۲].

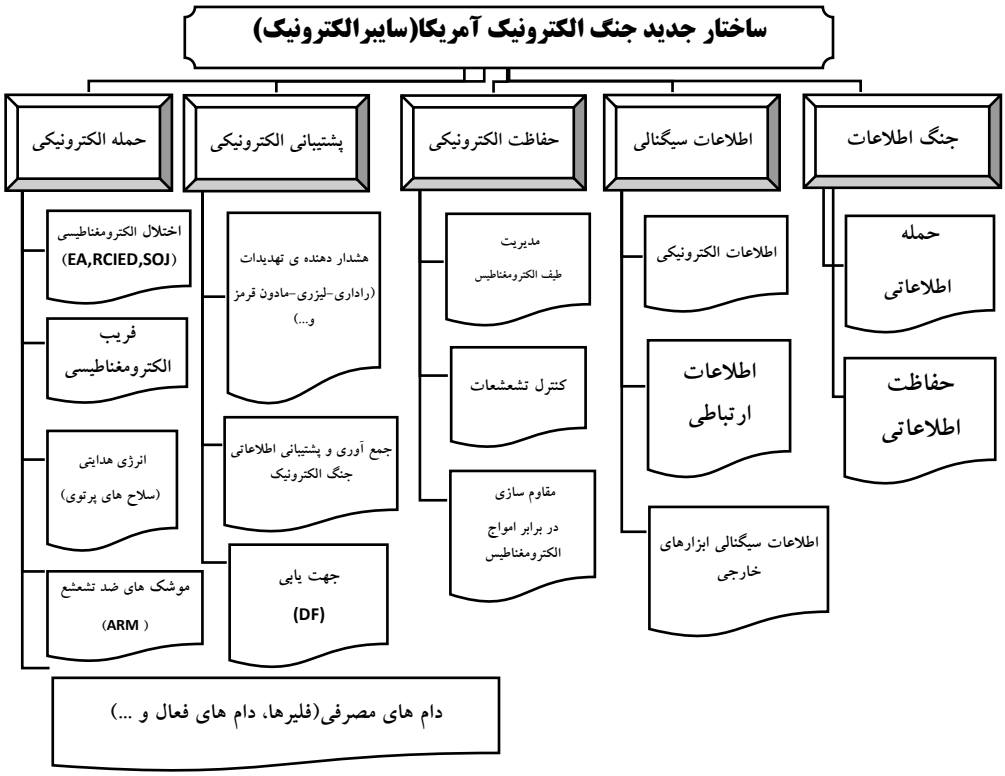
همگرایی و هم‌افزایی اطلاعات سیگنالی با جنگ سایبری و جنگ الکترونیک (سایبر الکترونیک)

از اهداف و اولویت‌های اولیه فرماندهی سایبری ارتش آمریکا، ایجاد قابلیت سایبر الکترونیک برای تأثیرگذاری در فضای سایبری به‌منظور پشتیبانی از عملیات جنگ الکترونیک است که به‌صورت هماهنگ و هم‌زمان توسط سازمان رزم در منطقه عملیاتی اجرا می‌گردد. عملیات شبکه، جنگ شبکه،

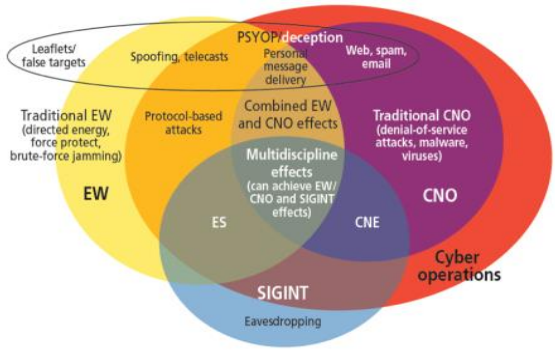
[1] Suppression of Enemy Air Defense(SEAD)

عملیات شبکه رایانه‌ای، برتری‌های فضائی، جنگ الکترونیک و اطلاعات سیگنالی ازجمله قابلیت‌های سایبر الکترونیک است که موردتوجه فرماندهان عملیات راه‌کنشی صحنه نبرد قرار دارد. ایجاد یکپارچگی در مدیریت موضوعات سایبری، طیف الکترومغناطیس و اطلاعات سیگنالی 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 اعلام‌خطر و هشداردهنده[2] در این فرآیند همکاری می‌نمایند.

نمودار ۱: ساختار جدید سازمان جنگ الکترونیک آمریکا با رویکرد تهدیدات نوین



[1] NETCOM
[2] REDCOM



شکل ۱: فضای سایبری الکترونیک در مأموریت جدید سایبری امریکا [۳]

جدول ۱: سامانه‌های مختلف جنگ الکترونیک و اطلاعات سیگنالی آمریکا در منطقه [۴]

سامانه	کاربرد	عراق	افغانستان	عمان	امارات	قطر	بحرین	عربستان	کویت	فضاپایه	دریاپایه	هواپایه	زمین پایه
PROPHET	اطلاعات سیگنالی و جنگ الکترونیک	X	X			X		X	X	X		X	X
TACJAM	اطلاعات ارتباطی و جنگ الکترونیک	X	X	X	X		X	X	X	X	X	X	X
TRAFFICJAM	جهت‌یابی و رهگیری ارتباطات	X	X	X	X		X	X			X	X	X
TEAMMETE	اطلاعات سیگنالی و جنگ الکترونیک	X	X	X	X		X	X	X				X
CESAS	سامانه حمله الکترونیکی و پشتیبانی الکترونیکی (EA&ES)	X	X		X				X		X	X	X
TRAILBLAZER	کنترل و رهگیری و اختلال الکترونیکی	X	X	X		X		X	X		X	X	X
AHFEWS	حمله الکترونیکی	X	X		X		X	X	X			X	X
SANDCRAB	اطلاعات سیگنالی و جنگ الکترونیک (ES&EA)	X	X					X	X			X	X
TRACHWOLF	اطلاعات سیگنالی و جنگ الکترونیک بررسی سیگنال‌های دیجیتالی	X	X					X	X	X	X	X	X
IEWCS(OLD)	حمله الکترونیکی و پشتیبانی الکترونیکی	X	X	X	X	X	X	X	X			X	X
IEWCS GBCS-H/L (NEW)	اطلاعات سیگنالی و جنگ الکترونیک	X				X			X				X
JSTARS AN/TSQ179B	سامانه حمله الکترونیکی به رادارها	X	X	X	X	X	X	X	X	X	X	X	X
TEAMPACK	اطلاعات سیگنالی و جنگ الکترونیک	X	X	X				X	X	X			X
RREP SS-3	اطلاعات سیگنالی	X	X										X

در سازمان واحدهای عمده نیروی زمینی تعداد ۳۵ نوع دستگاه مختلف به‌عنوان زیرسامانه‌های منـدرج

در جدول فوق وجود دارد. در واحدهای پروازی نیروهای مسلح آمریکا تعدادی سکوی پروازی مخصوص جمع‌آوری اطلاعات سیگنالی و اقدامات جنگ الکترونیک مانند آواکس، U2، EF18G، EA6B، E2C وجود دارد که اطلاعات جمع‌آوری‌شده توسط این سکوها با سایر منابع جمع‌آوری زمینی و فضایی تلفیق و مورداستفاده توسط نیروهای عملیاتی در منطقه مورداستفاده قرار می‌گیرد [۵].

ساختار سازمانی جنگ الکترونیک آمریکا

ساختار جدید جنگ الکترونیک آمریکا طبق سند ۲۰۰۷ و ۲۰۱۲ به شرح ذیل می‌باشد:

الف- اضافه نمودن سلاح‌های با انرژی هدایت‌شونده (سلاح‌های پرتوی)[1] به بخش حمله الکترونیکی که با استفاده از امواج رادیویی و لیزری، عملکرد تجهیزات را مختل و از بین می‌برد [۶].

ب- افزودن مقاوم‌سازی الکترومغناطیس[2] به بخش حفاظت الکترونیکی، که مأموریت آن فقط مقاوم‌سازی سامانه‌های الکترونیکی در برابر تابش سلاح‌های با انرژی هدایت‌شونده[3] می‌باشد تا تأثیرات این نوع سلاح‌های را، کاهش یا بی‌اثر نماید [۷].

ج- افزودن ساختار جنگ اطلاعاتی و سایبری به ساختار جنگ الکترونیک آمریکا و انجام جنگ اطلاعات و حملات سایبری و جنگ شبکه محور[4] در میدان نبرد سایبری و دیجیتالی می‌باشد [۸].

ساختار کنونی جنگ الکترونیک و اطلاعات سیگنالی ارتش آمریکا

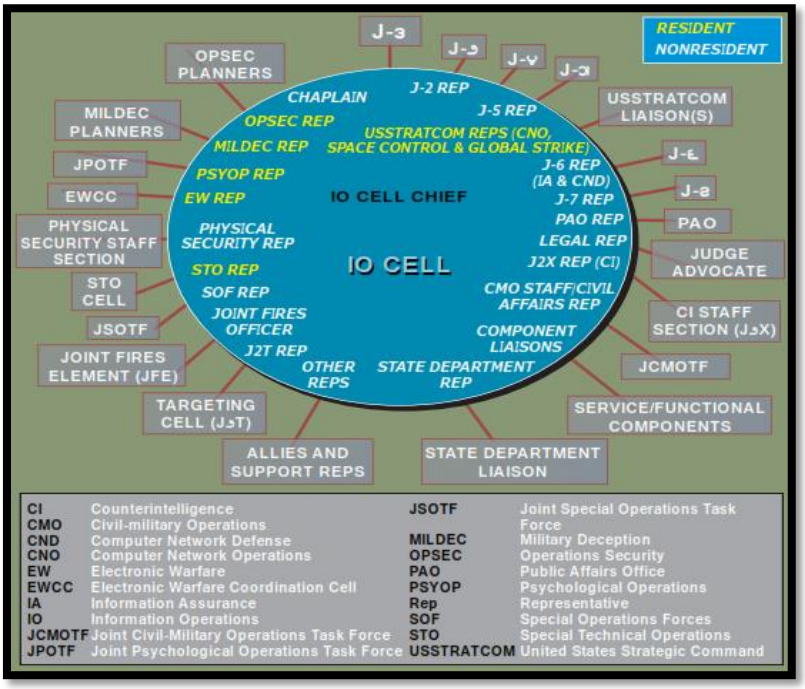
از سال ۱۹۹۹ تلاش مستمر برای ایجاد فرآیند یکپارچه‌سازی اطلاعات در ارتش امریکا آغاز گردید. "فرماندهی راهبردی ارتش امریکا"[5] کوشید تا سازمان و رده‌های مختلف اطلاعاتی را در قالب یک مجموعه واحد و منسجم اطلاعاتی تعریف و بکار گیرد. این مجموعه بنام "فرماندهی سایبری"[6] نامیده می‌شود و در آن سلول‌های اطلاعاتی متعددی ازجمله جمع‌آوری اطلاعات سیگنالی و جنگ الکترونیک ایفای نقش می‌کنند. این سلول‌ها پیکره و قالب اصلی عملیات اطلاعات را تشکیل می‌دهند. فعالیت‌های عملیات اطلاعات بر پشتیبانی از"فرماندهی نیروهای مشترک"[7] متمرکز گردیده است. هرچند که قابلیت عملیات اطلاعات در پنج محور اطلاعاتی یعنی"عملیات روانی"[8]،"عملیات فریب نظامی"[9]، "عملیات حفاظت اطلاعات"[10]، "عملیات شبکه رایانه‌ای"[11] و عملیات جنگ الکترونیک بیان شده است، اما نباید از قابلیت و توانمندی‌های سایر رده‌های اطلاعاتی در شکل‌گیری فرآیند عملیات اطلاعات غافل ماند. در سلول عملیات اطلاعات تعدادی از بخش‌ها به‌صورت ثابت و مقیم و تعدادی به‌صورت غیرمقیم

[1] DIRECTED ENERGY WEAPONS
[2] ELECTOMAGNETIC HARDENING
[3] DIRECTED ENERGY WEAPON(DEW)
[4] NETWORK CENTRIC WARFARE
[5] US STRATCOM
[6] CYBERCOM
[7] JFC
[8] PSYOPS
[9] MILDEC
[10] OPSEC
[11] CNO

ایفای نقش می‌نمایند. بخش‌های مقیم شامل بخش عملیات فنی، جنگ الکترونیک، عملیات روانی، حفاظت اطلاعات، عملیات فریب نظامی و عملیات راهبردی(عملیات شبکه، کنترل فضا و حمله گسترده و جهانی) است. نکته قابل‌توجه در این چینش این است که در عملیات اطلاعات امور فناورانه از امور غیرفناورانه جدا شده است.

بخش‌های حمله الکترونیک و دفاع الکترونیک مستقل از هم عمل می‌کنند. بخش عملیات روانی یکی از اعضای ثابت و مقیم در عملیات اطلاعاتی است و به عملیات شبکه‌ای و فضای سایبری به‌عنوان یک فعالیت محوری و عمده نگاه شده است. در سلول عملیات اطلاعات بخش‌های زیر به‌عنوان عناصر غیرمقیم ایفای نقش می‌نمایند بخش‌های امور مذهبی، طراحی و عملیات، اطلاعات، تدارکات، مالی، مخابرات، فعالیت‌های عمومی، حقوقی، ضداطلاعات، نگهداری، فعالیت درون‌شهری، تعیین اهداف، هدایت آتش، حفاظت فیزیکی، نیروی مخصوص، امور ایالتی و امور متفرقه. مدیر سلول اطلاعات با مسئولین هر یک از بخش‌های مقیم و غیرمقیم در اجرای عملیات اطلاعات هماهنگی می‌کند [۹].

شکل ۲: سلول عملیات اطلاعاتی آمریکا



دکترین جنگ الکترونیک آمریکا

نکات موردنظر در سند راهبردی دکترین جنگ الکترونیک آمریکا عبارت‌اند از:

۱. سامانه‌های جنگ الکترونیک می‌بایست اطلاعات جنگ الکترونیک مورداستفاده را به‌موقع و به هنگام در سطح تمام نیروهای عملیاتی توزیع نمایند.

۲. میادین نوین جنگ الکترونیک ازنظر فناوری پیچیده‌تر می‌شوند ولی عملیات نظامی همچنان در فضای پیچیده الکترومغناطیسی باید در جریان باشد ازاین‌رو فرماندهان و کارکنان می‌بایست به‌طور کامل از اثرات فضای الکترومغناطیسی بر عملیات آگاه بوده و همچنین از چگونگی بهره‌برداری از مزایای عملیات جنگ الکترونیک کشورهای همسو آگاهی کامل داشته باشند.

۳. لازم است کارگروه‌های جنگ الکترونیک در زمان عملیات متناسب با چارچوب سازمانی واحد عملیاتی ایجاد شود. تنها هدف گروه کاری جنگ الکترونیک حصول اطمینان از موفقیت با رعایت اصول یکپارچه‌سازی، عدم وجود تداخل در عملیات می‌باشد.

۴. جهت هماهنگی عملیات جنگ الکترونیک در بین نیروهای مشترک و چندملیتی، افسران جنگ الکترونیک می‌بایست از چارچوب سازمانی، روش‌ها و دستورالعمل‌ها آگاهی کامل داشته باشند.

۵. باید دسترسی آزاد به بخش‌های منتخب طیف الکترومغناطیس به‌منظور تأثیرگذاری بر سامانه تسلیحاتی دشمن و حفاظت از امکانات خودی در سرتاسر جهان فراهم گردد.

۶. جنگ الکترونیک یک قابلیت چندوجهی است و تجمیع اثرات آن با سایر فعالیت‌ها منجر به هم‌افزایی توانمندی‌ها و کاهش تلفات خواهد شد.

۷. کنترل طیف الکترومغناطیس عامل اساسی و حساس در موفقیت عملیات نظامی خواهد بود. بهره‌برداری از قابلیت جنگ الکترونیک نه‌تنها بر اساس یک رشته عملیات مشترک و اهداف عملی واقعی بلکه بر اساس توجه به خطرات محتمل در پاسخ‌های دشمن به عملیات است.

۸. به‌منظور انجام عملیات تجسسی یکنواخت لازم است از سامانه‌های جدید جمع‌آوری هوا پایه استفاده گردد.

۹. محیط عملیاتی جنگ الکترونیک شامل هوا، زمین، دریا، فضا و فضای سایبر خواهد بود.

۱۰. با استفاده از تسلیحات ماکرویو پرقدرت و سلاح‌های پرتوی بخشی از جنگ الکترونیک توسط نیروهای مسلح تعریف شده است.

۱۱. طراحان مشترک شش متغیر سیاسی، اجتماعی، اقتصادی، نظامی، اطلاعاتی و زیرساختی را در محیط عملیاتی موردتوجه قرار می‌دهند.

۱۲. اهداف الکترومغناطیسی شامل تسلیحات انفرادی، سامانه‌های تعیین موقعیت، اهداف زیرزمینی، تسلیحات انفجاری بزرگ، مخابراتی، تجاری، حساسه‌های هوایی و زیرزمینی، سامانه‌های فضاپایه، زمین پایه، سامانه‌های مخابراتی و شبکه‌های رایانه‌ای، موتورها و ژنراتورها و تأسیسات الکتریکی خواهد بود [۱۰].

فناوری‌های نوین جنگ الکترونیک مورداستفاده آمریکا

۱. استفاده از فناوری احتمال آشکارسازی کم[1] و احتمال رهگیری کم[2] در سامانه‌های رادارهای هوایی، زمینی و دریایی و به‌کارگیری رادارهای دو پایه[3]، چند پایه[4]، ماورای افق و ارائه فازی [۱۱].

۲. استفاده از فناوری پنهان‌کاری(شناساگریزی)[5] و پوشش در سامانه‌های راداری، ارتباطی و هواپیماهای مهاجم همانند F-117، U-2، F-22.

۳. برنامه‌ریزی هوشمند در به‌کارگیری گیرنده‌های بسیار پیشرفته، دقیق و هوشمند در جمع‌آوری اطلاعات سیگنالی در بخش پشتیبانی الکترونیکی در سکوهای هوایی(باسرنشین و بدون سرنشین)، زمینی، دریایی و فضایی(ماهواره‌ای) در منطقه با استفاده از سایت‌ها و پایگاه‌های مختلف در همسایگی ایران.

۴. استفاده از سامانه توزیع اطلاعات مشترک راه کنشی[6] در میدان نبرد دیجیتالی.

۵. توان تأثیرگذاری بالا بر میدان نبرد، با استفاده از موشک‌های هوشمند کروز پرسه‌زن، نفوذگر[7] و کف رو[8] و موشک‌های ضد تشعشع امواج راداری[9].

۶. استفاده از سامانه‌های ضد فضایی[10] و به‌کارگیری هواپیماهای جنگ الکترونیک F-117A،EA6، F-22، B-3،B-2 ، JSTAR،(E3Y،E2C) مجهز به پادهای هوشمند و پیشرفته با فناوری‌های نوین حمله الکترونیکی عمل پارازیت‌رسانی به‌صورت دفاع از خود، حفاظت از دسته‌های پروازی و دور ایستا [۱۲].

۷. توانایی اختلال بر روی رادارهای با روزنه‌ی ترکیبی و روزنه ترکیبی معکوس (SAR/ISAR).

۸. استفاده از هوش مصنوعی و رباتیک در تجهیزات جنگ الکترونیک به‌منظور بالا بردن دقت و سرعت عمل [۱۳].

۹. استفاده از فناوری‌های حفاظت الکترونیکی پیشرفته راداری و ارتباطی در آمریکا همانند؛ فناوری‌های حفاظت الکترونیکی القایی و تخصیصی در رادارهای جستجوگر و هدف‌یاب و فناوری‌های حفاظت الکترونیکی القایی و تخصیصی در رادارهای ردیاب و همچنین فناوری‌های حفاظت الکترونیکی در سامانه‌های ارتباطی [۱۴].

۱۰. استفاده از انواع مختلف پهپادهای؛ پری‌دیتور، گلوبال‌هاک، دارک‌استارو غیره مجهز به تجهیزات جنگ الکترونیک همانند شناسایی، مراقبت، هدف زنی، رله‌های ارتباطی و پادهای اخلالگر، سامانه‌های رادار با روزنه ترکیبی و حساسه‌های سنجشی و علائمی (مسینت)، اطلاعات سیگنالی و ردیاب‌های مادون‌قرمز، لیزری [۱۵].

۱۱. استفاده بیش از ۲۰۰ ماهواره در بخش اطلاعاتی در دنیا وجود دارد که قسمت اعظم آن اطلاعات

---

[1] LOW PROBABILITY OF DETECTION (LPD)
[2] LOW PROBABILITY OF INTERCEPT (LPI)
[3] BI-STATIC
[4] MULTI STATIC
[5] STEALTH
[6] JTIDS
[7] PENETRATING CRUISE MISSILE
[8] SEA SKIMMING MISSILE
[9] ANTI-RADIATION MISSILE (ARM)
[10] SPACE COUNTER

موردنیاز برای قسمت‌های مختلف جنگ الکترونیک را جمع‌آوری و در اختیار آمریکا قرار می‌دهند، ازجمله ماهواره‌های کنیون، ورتکس، مرکوری، ترومپت [۱۶].

۱۲. به‌کارگیری بمب‌های خوشه‌ای[1]، بمب‌های الکترومغناطیسی و بمب‌های لیزری.

۱۳. استفاده از سامانه‌های هوشمند جمع‌آوری اطلاعات با استفاده از گیرنده‌ها و سامانه‌های اکتشافی شناسایی و هشداردهنده همانند؛ گیرنده‌های اکتشافی یا شناسایی در بخش پشتیبانی الکترونیکی همانند؛ گیرنده کریستالی تصویری، سوپرهترودواین، میکرواسکن، اندازه‌گیری آنی فرکانس، صوتی-تصویری براگسل و گیرنده‌های دیجیتالی که قادر است تا فرکانس ۱۱۰ گیگاهرتز را آشکارسازی نمایند و گیرنده‌های هشداردهنده راداری[2]، هشداردهنده لیزری[3]، هشداردهنده مادون‌قرمز[4]، هشداردهنده پرتاب موشک[5]، هشداردهنده نزدیک شدن موشک و سامانه‌های مادون‌قرمز روبه‌جلو[6] برای شناسایی و هشدار تهدیدات میدان نبرد استفاده می‌گردد [۱۷].

۱۴. توانائی اختلال بر روی طیف الکترومغناطیس تا ۳۰۰ گیگاهرتز در بخش‌های مختلف که نمونه‌ای از آن در سند ۲۰۰۷ و ۲۰۱۲ دکترین جنگ الکترونیک آمریکا آمده است.

۱۵. آمریکا با امکانات ضدهوایی و در اختیار داشتن تجهیزات مختلف، مانع استفاده و دسترسی دیگران به قلمرو هوایی با استفاده از هواپیماهای مجهز به سلاح‌های لیزری و سلاح‌های ماکروویوی با قدرت بالا[7] (سلاح‌های پرتوی) می‌گردد [۱۸].

۱۶. امکانات ضدفضایی ماهواره‌های کشنده مجهز به سلاح‌های لیزری ماکروویوی و انرژی جنبشی(سلاح‌های پرتوی) می‌باشند و قادر هستند آن‌ها را به سمت ماهواره‌ها گسیل و باعث از کار انداختن آن‌ها گردند [۱۹].

فناوری‌های علمی و پژوهشی جنگ الکترونیک آمریکا

۱. با مطالعه و بررسی پروژه‌های در دست اقدام و آتی آمریکا در زمینه جنگ الکترونیک در سندهای AIR FORCE 2025، JUANERY 25 ELECTRONIC WARFARE JOINT PUBLICATION 3-13.1، 2007 JOINT DOCTRINE FOR ELECTRONIC WARFARE 7 ۳-۵۱JOINT PUBLICATION APRIL 2000، که چشم‌انداز ۳۰ سال آینده نیروی هوایی این کشور را در بردارد، خلاصه استخراج‌شده آن شامل؛ استفاده از موشک‌های پرسه‌زن[8]، حملات برد بلند موشکی، موشک‌های کروز راه‌کنشی با حسگرهای (مادون‌قرمز، لیزری و راداری)، پهپاد حامل موشک‌های فوق هوشمند[9]، مهمات با اثرات ترکیبی، بمب‌های با قطر کوچک، هواپیمای تهاجمی مافوق صوت، هواپیمای پنهان‌کار باسرنشین و

[1] CLUSTER BOMB
[2] RADAR WARNING RECEIVER (RWR)
[3] LASER WARNING RECEIVERS (LWR)
[4] INFRA RED WARNING RECEIVER(IRWR)
[5] MISSILE LAUNCH WARNER/MISSILE APPROCH WARNER (MLW/ MAW)
[6] FORWARD LOOKING INFRARED SYSTEMS (FLIR)
[7] HIGH POWER MICROWAVE (HPM)
[8] LOITERING ATTACK MISSILE
[9] LOCAAS

بدون سرنشین، هواپیمای پنهان‌کار فتوفایتر[1]، مجموعه ماهواره‌های نگهبان، سامانه توهم‌زای تصویری هوایی[2] می‌باشد.

۲. استفاده از عملیات سخت کشنده[3] جنگ الکترونیک با استفاده از سلاح‌های پرتوی و موشک‌های ضد تشعشعی و عملیات نرم کشنده[4] با استفاده از انواع تکنیک‌های اختلال و فریب توسط پادهای هواپیماهای مختلف انجام می‌شود.

۳. یکی از مهم‌ترین راهبردهای قرن ۲۱ آمریکا، جنگ اطلاعات و حملات سایبری و انجام جنگ شبکه محور[5] در میدان نبرد سایبری و دیجیتالی می‌باشد و طبق آماری که از فرماندهی دفاع سایبری در جهان منتشر کرد. روزانه ۵۵۰۰۰ بدافزار (ویروس) در جهان تولید و منتشر می‌شود که از این میان برخی از آن‌ها در حوزه مقابله با امنیت سایر کشورها به‌خصوص ایران بکار گرفته می‌شود. ویروس‌هایی همانند استاکس‌نت[6] علیه تأسیسات اتمی ایران از این قبیل بدافزار می‌باشند [۲۰].

فناوری‌های جنگ الکترونیک آمریکا در جنگ‌های احتمالی

۱. جمع‌آوری اطلاعات هوشمند در بخش پشتیبانی الکترونیکی جهت تأمین اطلاعات موردنیاز بخش حفاظت الکترونیکی و حمله الکترونیکی از زمین، دریا، هوا و فضا و فضای سایبری.

۲. مراقبت، شناسایی و فرماندهی و کنترل از زمین، هوا، فضا، دریا و فضای سایبری با استفاده از مرکز فرماندهی و کنترل(سنتکام) در کشورهای منطقه ازجمله قطر.

۳. استفاده از سامانه دفاع هوایی ایجیس[7] در دریا با پشتیبانی ناوهای هواپیمابر در خلیج‌فارس و دریای عمان، پایگاه‌های نظامی کشورهای همسایه ایران و ماهواره‌ها از فضا.

۴. استفاده از هواپیماهای دورایستا از قبیل آواکس، JSTAR،RC135 و سایر هواپیماهای اطلاعات سیگنالی در منطقه ایستایی[8] جهت جمع‌آوری اطلاعات، مراقبت و شناسایی[9].

۵. عملیات جنگ الکترونیک دور ایستا[10] با استفاده از موشک‌های کروز با برد بیش از ۲۵۰۰ کیلومتر و موشک‌های کروز پرسه‌زن و پهپادهای پیشرفته همچون (پریدیتور، دارک‌استار، گلوبال‌هاک و....) و هواپیماهای B-2، B52، JSTAR، F-22، F-117.

۶. عملیات اختلال و فریب جنگ الکترونیک با استفاده از حملات هوایی توسط هواپیماهای جنگ الکترونیک S3، EF18، EA6 (و سایر هواپیماهای جنگ الکترونیک به همراه هواپیماهای شکاری و بمب‌افکن راه‌کنشی).

[1] FOTO- FIGHTER
[2] AIRBONE HOLOGRAPHIC PROJECTOR
[3] HARD KILL
[4] SOFT KILL
[5] NETWORK CENTRIC WARFARE
[6] STUXNET
[7] AEGIS
[8] Holding
[9] Information , Surveillance, Reconnaissance (ISR)
[10] STAND OFF JAMMER

۷. بهره‌برداری و استفاده از تسلیحات حامل انرژی هدایت‌شونده(سلاح‌های پرتوی) و موشک‌های ضد تشعشعی علیه سامانه‌های راداری و ارتباطی.
۸. استفاده از مهمات هوشمند در عملیات‌های هوایی، زمینی و دریایی.
۹. طرح‌ریزی و اجرای حملات سایبری بر روی سامانه‌های رایانه‌ای، ارتباطی، راداری، فرماندهی و کنترل، مراکز داده‌های زیرساخت‌های حیاتی، حساس و مهم [۲۱].

توانمندی‌های فناوری‌های جنگ الکترونیک کشور

۱. نهادینه‌سازی آموزش‌های جنگ الکترونیک در نیروهای مسلح در مقاطع تحصیلی کارشناسی، کارشناسی ارشد و دکتری با استفاده از تشکیل رشته آموزشی جنگ الکترونیک در دانشگاه هوایی شهید ستاری(کارشناسی و کارشناسی ارشد)، دانشگاه امام حسین(ع) (دکتری)و دانشگاه فرماندهی و ستاد آجا (کارشناسی ارشد) و سایر مراکز آموزشی و عملیاتی) و آموزش به سایر رشته‌های مرتبط در دانشگاه‌های غیرنظامی.
۲. بهره‌برداری، به‌کارگیری، بومی‌سازی و مهندسی معکوس تجهیزات جنگ الکترونیک شرقی و غربی موجود در نیاجا با استفاده از بنیه‌ی علمی، پژوهشی و عملیاتی دانشگاه‌های نظامی، غیرنظامی و بخش صنعت کشور.
۳. طراحی، ساخت و به‌کارگیری سامانه‌های جمع‌آوری اطلاعات بومی و هوشمند پشتیبانی الکترونیکی به‌منظور تشخیص دقیق و آنی تهدیدات طیف الکترومغناطیس دشمن.
۴. برگزاری همایش و کنفرانس سالانه جنگ الکترونیک با همکاری دانشگاه‌های نظامی و غیرنظامی و نهادینه شدن فرهنگ جنگ الکترونیک در نیاجا.
۵. طراحی، ساخت و ارتقاء و بهینه‌سازی تجهیزات جنگ الکترونیک توسط جهاد خودکفایی نیاجا و وزارت دفاع و بخش صنعت.
۶. تشکیل فرماندهی جنگ الکترونیک در نیاجا به‌منظور رصد و پایش تهدیدات و اقدام راه‌کنشی عملیاتی و راهبردی دشمن [۲۲].

۲-۲ پیشینه‌های پژوهش

مشابه موضوع مقاله‌ی مذکور در دانشگاه‌های داخل و خارج کشور انجام نشده است، ولی عناوین رساله‌ها و تحقیقات مرتبط با متغیرهای موردنظر در مقاله مذکور به شرح ذیل می‌باشد:

(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 تهدیدات حوزه اطلاعات هوایی، که مهم‌ترین نتایج حاصله عبارت‌اند از: بهره‌گیری از توان صنایع مرتبط در ایجاد اختلال در رایانه‌های دشمن از طریق سوابق اطلاعاتی و تهیه نرم‌افزار رایانه‌ای، استفاده جهت‌دار دانش نخبگان به‌منظور شناسایی حساسه‌های سنجشی و علائمی (مسینت) و جنگ اطلاعات، بهره‌گیری از توان علمی نخبگان به‌منظور ایجاد اختلال در به‌کارگیری رایانه توسط دشمن و کاهش کارایی و عدم دسترسی او به اطلاعات در

عمق کشور از طریق تهیه نرم‌افزارها، به‌کارگیری تجربه نسبتاً بالای جمع‌آوری اطلاعات به‌منظور محدود نمودن دسترسی دشمن به اطلاعات تاکتیکی از طریق سوابق موجود، تقویت آموزش اطلاعات به‌منظور دریافت تاکتیک‌های ضدشنود دشمن، به‌کارگیری توان رهگیری مستمر اطلاعات و تجربه بالای جمع‌آوری اطلاعات، ایجاد هماهنگی‌های مؤثر درون‌سازمانی و برون‌سازمانی و همچنین اصلاح مدیریت اطلاعات به‌منظور کاهش دسترسی دشمن به اطلاعات تاکتیکی و راهبردی در عمق از طریق تشکیل کارگروه‌های تخصصی، به‌کارگیری قابلیت‌های صنایع در ارسال اطلاعات مجازی به‌منظور اشباع شبکه اطلاعاتی دشمن او از طریق نفوذگرها [۲۳].

(۲) پروژه تحقیقاتی"جمع‌آوری، تحلیل و پردازش اطلاعات سامانه‌های جنگ الکترونیک ارتش آمریکا مستقر در خلیج‌فارس" با هدف اصلی، ارائه اطلاعات سامانه‌های جنگ الکترونیک و اطلاعات سیگنالی یگان‌های ارتش آمریکا مستقر در منطقه خلیج‌فارس در سه سطح راهکنشی، عملیاتی و راهبردی، که مهم‌ترین نتایج حاصله عبارت‌اند از؛ کوچک و کیفی‌سازی سازمان اطلاعات سیگنالی و جنگ الکترونیک، تجهیز و آماده‌سازی در رده‌های کوچک‌تر، برخورداری از ساختار تجزیه‌وتحلیل 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 سیگنالی و جنگ الکترونیک چندمنظوره‌ی کم‌حجم 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 [۲۴].

۳. روش‌شناسی پژوهش

این پژوهش ازنظر هدف کاربردی، توسعه‌ای و روش تحقیق آمیخته از نوع موردی-زمینه‌ای، روش گردآوری اطلاعات کتابخانه‌ای با مطالعه اسناد و مدارک موجود و ابزار آن بررسی اسناد و مدارک، آرشیو، کتاب، رساله دکتری، استفاده از اطلاعات موجود در وبگاه اینترنت و مصاحبه با استفاده از پرسش‌نامه جهت اخذ نظر خبرگان می‌باشد. به‌منظور تجزیه‌وتحلیل و ارائه راهبردها از روش نوین تدوین راهبرد استفاده و سپس با استفاده از روش خبرگی عوامل محیطی(قوت، ضعف، تهدیدها و فرصت‌ها) احصاء و با استفاده از ماتریس SWOT جهت تدوین راهبرد و استفاده از نرم‌افزار TOPSIS در تعیین اولویت راهبردهای و سپس اقدام به تجزیه‌وتحلیل اطلاعات شده است. قلمرو زمانی پژوهش تهدیدهای از قبل تا پنج سال آتی در افق چشم‌انداز ۱۴۰۴ می‌باشد. قلمرو مکانی سامانه‌های جنگ الکترونیک، راداری و ارتباطی دو کشور جمهوری اسلامی ایران و آمریکا می‌باشد. جامعه آماری۴۰ نفر به‌صورت تمام شمار، شامل صاحب‌نظران، خبرگان و نخبگان، متخصصان، کارشناسان و اساتید دانشگاه در حوزه‌های جنگ الکترونیک که حداقل دارای ۱۵سال سابقه اجرایی و مدیریتی و حداقل دارای

مدرک تحصیلی کارشناسی ارشد (۶۵٪ دکتری و ۳۵٪ کارشناسی ارشد) می‌باشد. روایی پرسش‌نامه به تائید خبرگان و اساتید دانشگاه رسیده و پایایی آن با آزمون آلفای کُرُنباخ ۰/۸۶ بوده که نشانگر پایایی پرسش‌نامه می‌باشد.

۴. تجزیه و تحلیل یافته‌ها

۴-۱ ماتریس ارزیابی عوامل داخلی (IFE)

جهت تحلیل محیط با تهیه پرسش‌نامه و دریافت نقطه‌نظر خبرگان جنگ الکترونیک و با توجه به عوامل اصلی و اثرگذار ماتریس موردنظر و ارزش‌گذاری آنان نقاط قوت و ضعف خودی و فرصت‌ها و تهدیدهای دشمن به شرح ذیل احصاء گردید:

جدول ۲: نقاط قوت جنگ الکترونیک نپاجا حاصل از یافته‌های تحقیق

قوت	نقاط قوت حاصل از یافته‌های تحقیق
S1	برخورداری از حمایت‌ها و تأکیدات مقام معظم رهبری در حوزه‌ی جنگ الکترونیک.
S2	تشکیل فرماندهی جنگ الکترونیک در نپاجا جهت رصد، پایش و اقدام در برابر تهدیدات.
S3	قابلیت طراحی، ساخت و به‌کارگیری تجهیزات جنگ الکترونیک بومی در نپاجا.
S4	قابلیت طراحی، ساخت، ارتقاء و بومی‌سازی تجهیزات جنگ الکترونیک در وزارت دفاع و صنایع غیرنظامی کشور.
S5	وجود بنیه علمی بسیار مناسب در دانشگاه‌های نظامی، غیرنظامی و صنایع کشور در حوزه جنگ الکترونیک.
S6	تشکیل فرماندهی جنگ الکترونیک راهبردی در آجا.
S7	اجرای رزمایش‌های تخصصی مشترک جنگ الکترونیک.
S8	اجرای آموزش جنگ الکترونیک در مقاطع کارشناسی ، کارشناسی ارشد و دکتری در سطح آجا و نیروهای مسلح.
S8	وجود شبکه فرماندهی و کنترل یکپارچه بومی در نپاجا.

جدول ۳: مقادیر عددی نقاط قوت دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره قوت	تطابق با عامل							وضع موجود(اهمیت)					میانگین(ضریب اهمیت)	نمره موزون عامل
	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها						
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
S1	۰	۱۳	۱۶	۷	۴	۲/۰۳۳۳۳	۰/۰۴۹۷۵۵	۰	۱۲	۲۱	۴	۳	۱/۹۶۶۶۶۷	۰/۰۹۷۸۵۲
S2	۰	۱۴	۲۰	۴	۲	۱/۹	۰/۰۴۶۴۹۳	۰	۱۴	۱۸	۶	۲	۱/۹۳۳۳۳۳	۰/۰۸۹۸۸۶
S3	۰	۱۲	۲۲	۴	۲	۱/۹۳۳۳۳۳	۰/۰۴۷۳۰۸	۰	۱۵	۱۴	۸	۳	۱/۹۸۳۳۳۳	۰/۰۹۳۸۲۸
S4	۰	۱۱	۲۵	۲	۲	۱/۹۱۶۶۶۷	۰/۰۴۶۹	۰	۲۱	۱۵	۳	۱	۱/۷۳۳۳۳۳	۰/۰۸۱۲۹۴
S5	۰	۱۰	۲۳	۵	۲	۱/۹۸۳۳۳۳	۰/۰۴۸۵۳۲	۰	۱۸	۱۷	۴	۱	۱/۸	۰/۰۸۱۲۹۴
S6	۰	۱۳	۲۱	۳	۳	۱/۹۳۳۳۳۳	۰/۰۴۷۳۰۸	۰	۱۶	۱۷	۵	۲	۱/۸۳۳۳۳۳	۰/۰۸۹۰۹۷
S7	۰	۱۱	۱۸	۸	۳	۲/۰۵	۰/۰۵۰۱۶۳	۰	۱۸	۱۵	۶	۱	۱/۸۳۳۳۳۳	۰/۰۹۱۹۶۶
S8	۰	۱۸	۱۹	۲	۱	۱/۷۶۶۶۶۷	۰/۰۴۳۲۳	۰	۱۷	۱۹	۲	۲	۱/۸۱۶۶۶۷	۰/۰۷۸۵۳۵
جمع						۱۵/۵۱۶۶۷	۰/۳۷۹۶۹						۱۴/۹۴۹۹۹۹	۰/۷۰۹۸۱۵

جدول ۴: نقاط ضعف دفاع سایبری کشور حاصل از یافته‌های تحقیق

ضعف	نقاط ضعف حاصل از یافته‌های تحقیق
W1	بومی نبودن برخی از سامانه‌های جنگ الکترونیک نپاجا
W2	نبود گیرنده‌های هشداردهنده لیزری و مادون‌قرمز در برخی از تجهیزات خودی
W3	کافی نبودن فناوری احتمال رهگیری کم و احتمال آشکارسازی کم در برخی از سامانه‌های راداری نپاجا
W4	کافی نبودن فناوری طیف گسترده در برخی از سامانه‌های ارتباطی نپاجا
W5	آسیب‌پذیری سامانه‌های مورداستفاده در طیف الکترومغناطیس نپاجا در برابر تهدیدات سلاح‌های پرتوی[1] (لیزری و ماکروویو)، بمب‌های الکترومغناطیس، موشک‌های کروز و موشک‌های ضدتشعشع و تهدیدات سایبری دشمن
W6	آسیب‌پذیری نسبی برخی از سامانه‌های طیف الکترومغناطیس نپاجا در برابر برخی از حملات الکترونیکی دشمن
W7	شناسایی و موقعیت‌یابی آرایش نظامی الکترونیکی نپاجا توسط دشمن
W8	ضعف نسبی در رهگیری و شناسایی برخی هواپیماهای پنهان‌کار باسرنشین و بدون سرنشین
W9	عدم برخورداری از سامانه اختلال‌گر دورایستا زمینی و هوایی

[1] – Directed Energy Weapon (DEW)

جدول ۵: مقادیر عددی نقاط ضعف دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره قوت	تطابق با عامل							وضع موجود(اهمیت)					میانگین(ضریب اهمیت)	نمره موزون عامل
	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها						
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
W1	۰	۰	۶	۲۲	۱۲	۲/۷۶۶۶۶۷	۰/۰۶۷۷	۰	۰	۱۱	۱۵	۱۴	۲/۷۱۶۶۶۷	۰/۱۸۳۹۱۸
W2	۰	۰	۷	۱۵	۱۸	۲/۸۵	۰/۰۶۹۷۳۹	۰	۰	۳	۱۵	۲۲	۲/۹۸۳۳۳۳	۰/۲۰۸۰۵۵
W3	۰	۰	۷	۱۷	۱۶	۲/۸۱۶۶۶۷	۰/۰۶۸۹۲۳	۰	۰	۳	۱۲	۲۵	۳/۰۳۳۳۳۳	۰/۲۰۹۰۶۷
W4	۰	۰	۹	۱۷	۱۴	۲/۷۵	۰/۰۶۷۲۹۲	۰	۰	۳	۱۶	۲۱	۲/۹۶۶۶۶۷	۰/۱۹۹۶۳۳
W5	۰	۰	۶	۱۹	۱۵	۲/۸۱۶۶۶۷	۰/۰۶۸۹۲۳	۰	۰	۲	۱۶	۲۲	۳	۰/۲۰۶۷۷
W6	۰	۰	۸	۱۵	۱۷	۲/۸۱۶۶۶۷	۰/۰۶۸۹۲۳	۰	۰	۲	۱۷	۲۱	۲/۹۸۳۳۳۳	۰/۲۰۵۶۲۱
W7	۰	۰	۶	۱۶	۱۸	۲/۸۶۶۶۶۷	۰/۰۷۰۱۴۷	۰	۰	۲	۱۷	۲۱	۲/۹۸۳۳۳۳	۰/۲۰۹۲۷۱
W8	۰	۰	۷	۱۷	۱۶	۲/۸۱۶۶۶۷	۰/۰۶۸۹۲۳	۰	۰	۴	۱۳	۲۳	۲/۹۸۳۳۳۳	۰/۲۰۵۶۲۱
W9	۰	۰	۵	۱۹	۱۶	۲/۸۵	۰/۰۶۹۷۳۹	۰	۰	۲	۱۴	۲۴	۳/۰۳۳۳۳۳	۰/۲۱۱۵۴۲
جمع						۲۵/۳۵۰۰۲	۰/۶۲۰۳۰۹						۲۶/۶۸۳۳۳	۱/۸۳۹۴۹۸
جمع قوت و ضعف						۴۰/۸۶۶۶۷	۱						۴۱/۶۳۳۳۳	۲/۵۴۹۳۱۳

جدول ۶: خلاصه ماتریس عوامل داخلی (IFE)

عوامل محیط داخلی	میانگین موافقت	وزن عامل	میانگین وضع موجود (ضریب اهمیت)	نمره موزون
قوت‌ها	۱۵/۵۱۶۶۷	۰/۳۷۹۶۹	۱۴/۹۴۹۹۹۹	۰/۷۰۹۸۱۵
ضعف‌ها	۲۵/۳۵۰۰۰۲	۰/۶۲۰۳۱	۲۶/۶۸۳۳۳	۱/۸۳۹۴۹۸
مجموع قوت‌ها و ضعف‌ها	۴۰/۸۶۶۶۷۲	۱	۴۱/۶۳۳۳۲۹	۲/۵۴۹۳۱۳

بر اساس نتایج حاصله، چون عدد ضعف‌ها بیشتر از عدد قوت‌ها می‌باشد، بنابراین‌که جنگ الکترونیک نپاجا در محیط داخلی با ضعف روبرو است.

۴-۲ ماتریس ارزیابی عوامل خارجی (EFE)

جدول ۷: نقاط فرصت دفاع سایبری کشور حاصل از یافته‌های تحقیق

فرصت	نقاط فرصت حاصل از یافته‌های تحقیق
O1	قابلیت فریب و انحراف موشک‌های لیزری، موشک‌های ضدتشعشعی و موشک‌های کروز دشمن
O2	امکان حمله و فریب الکترونیکی سامانه‌های راداری و ارتباطی دشمن
O3	امکان رهگیری و شناسایی نسبی هواپیماهای پنهان‌کار باسرنشین و بدون سرنشین دشمن
O4	امکان شناسایی الکترونیکی کلیه فعالیت‌های راداری و ارتباطی دشمن
O5	امکان حفاظت الکترونیکی سامانه‌های راداری و ارتباطی خودی در برابر سلاح‌های پرتوی دشمن
O6	وابستگی بیش‌ازحد سامانه‌های راداری و ارتباطی دشمن به زیرساخت‌های سایبری و آسیب‌پذیر بودن آنان در برابر حملات الکترونیکی و سایبری(سایبر الکترونیک)
O7	امکان حمله الکترونیکی و سایبری بر روی شبکه‌های فرماندهی و کنترل دشمن در منطقه
O8	قابلیت شناسایی آرایش نظامی الکترونیکی دشمن در منطقه توسط نپاجا
O9	استفاده از جنگ‌های الکترونیک کلاسیک توسط دشمن و ضعف در استفاده از جنگ‌های ناهمتراز

جدول ۸: مقادیر عددی نقاط فرصت دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره ضعف	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها					میانگین(ضریب اهمیت)	نمره موزون عامل
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
O1	۰	۰	۲	۲۱	۱۷	۲/۹۱۶۶۶۷	۰/۰۵۶	۰	۸	۲۰	۱۱	۱	۲/۰۸۳۳۳۳	۰/۱۱۶۶۶۷
O2	۰	۰	۵	۱۸	۱۷	۲/۸۶۶۶۶۷	۰/۰۵۵۰۴	۰	۵	۲۱	۱۲	۲	۲/۱۸۳۳۳۳	۰/۱۲۰۱۷۱
O3	۱	۲	۷	۱۶	۱۴	۲/۶۶۶۶۶۷	۰/۰۵۱۲	۲	۶	۲۰	۱۱	۱	۲/۰۵	۰/۱۰۴۹۶
O4	۰	۰	۷	۱۸	۱۵	۲/۸	۰/۰۵۳۷۶	۱	۷	۱۶	۱۴	۲	۲/۱۵	۰/۱۱۵۵۸۴
O5	۰	۳	۵	۱۷	۱۵	۲/۷۳۳۳۳۳	۰/۰۵۲۴۸	۱	۶	۱۴	۱۶	۳	۲/۲۳۳۳۳۳	۰/۱۱۷۲۰۵
O6	۱	۳	۸	۱۴	۱۴	۲/۶۱۶۶۶۷	۰/۰۵۰۲۴	۱	۶	۱۴	۱۳	۶	۲/۲۸۳۳۳۳	۰/۱۱۴۷۱۵
O7	۰	۲	۱۱	۱۱	۱۶	۲/۶۸۳۳۳۳	۰/۰۵۱۵۲	۱	۵	۱۵	۱۵	۴	۲/۲۶۶۶۶۷	۰/۱۱۶۷۷۹
O8	۰	۰	۶	۱۸	۱۶	۲/۸۳۳۳۳۳	۰/۰۵۴۴	۱	۷	۱۴	۱۶	۲	۲/۱۸۳۳۳۳	۰/۱۱۸۷۷۳
O9	۰	۰	۷	۱۶	۱۷	۲/۸۳۳۳۳۳	۰/۰۵۴۴	۲	۶	۱۲	۱۷	۳	۲/۲۱۶۶۶۷	۰/۱۲۰۵۸۷
جمع						۲۴/۹۵	۰/۴۷۹۰۴						۱۹/۶۵	۱/۰۴۵۴۴

جدول ۹: نقاط تهدید دفاع سایبری کشور حاصل از یافته‌های تحقیق

تهدید	نقاط تهدید حاصل از یافته‌های تحقیق
T1	به‌کارگیری جنگ‌های شبکه محور و سایبری توسط دشمن
T2	به‌کارگیری بمب‌های الکترومغناطیسی و سلاح‌های پرتوی توسط دشمن
T3	به‌کارگیری موشک‌های کروز پرسه‌زن ضدرادار توسط دشمن
T4	استفاده از هواپیماهای پنهان‌کار و پیشرفته و هوشمند باسرنشین و بدون سرنشین توسط دشمن
T5	تمرکز دشمن بر حملات همگرای هوشمند سایبر الکترونیک
T6	حمله الکترونیکی با استفاده از هواپیماهای دورایستای جنگ الکترونیک (همانند هواپیمای جی‌استار- آواکس و...)
T7	به‌کارگیری بمب‌های الکترومغناطیسی، بمب‌های لیزری سلاح‌های پرتوی، موشک‌های کروز پرسه‌زن، موشک‌های ضدتشعشعی توسط دشمن
T8	استفاده از حسابه‌های پیشرفته اکتشافی- شناسایی هوشمند و حسابه‌های هشداردهنده(راداری، لیزری، مادون‌قرمز) در سامانه‌های هوایی، زمینی، دریایی و فضایی با هدف جمع‌آوری اطلاعات عملیاتی، تاکتیکی و راهبردی
T9	استفاده از فناوری‌های نوین راداری (رادار دوپایه و چندپایه، رادار ماورای افق، رادار با روزنه ترکیبی، ارائه فازی، رهگیری کم و آشکارسازی کم و...) و فناوری‌های نوین ارتباطی (طیف گسترده، ضدشنود) توسط دشمن

جدول ۱۰: مقادیر عددی تهدیدهای دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره ضعف	تطابق با عامل							وضع موجود(اهمیت)					میانگین(ضریب اهمیت)	نمره موزون عامل
	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها						
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
T1	۰	۰	۵	۱۰	۵	۳	۰/۰۵۷۶	۰	۰	۴	۱۶	۲۰	۲/۹۳۳۳۳۳	۰/۱۶۸۹۶
T2	۰	۰	۲	۱۶	۲۲	۳	۰/۰۵۷۶	۰	۰	۴	۱۴	۲۲	۲/۹۶۶۶۶۷	۰/۱۷۰۸۸
T3	۰	۰	۱	۱۶	۲۳	۳/۰۳۳۳۳۳	۰/۰۵۸۲۴	۰	۲	۳	۱۲	۲۳	۲/۹۳۳۳۳۳	۰/۱۷۰۸۳۷
T4	۰	۰	۵	۱۴	۲۱	۲/۹۳۳۳۳۳	۰/۰۵۶۳۲	۰	۱	۵	۱۲	۲۲	۲/۹۱۶۶۶۷	۰/۱۶۴۲۶۷
T5	۰	۰	۰	۱۷	۲۳	۳/۰۵	۰/۰۵۸۵۶	۰	۲	۴	۱۲	۲۲	۲/۹	۰/۱۶۹۸۲۴
T6	۰	۰	۳	۱۱	۲۶	۳/۰۵	۰/۰۵۸۵۶	۰	۰	۲	۱۸	۲۰	۲/۹۶۶۶۶۷	۰/۱۷۳۷۲۸
T7	۰	۰	۱	۱۶	۲۳	۳/۰۳۳۳۳۳	۰/۰۵۸۲۴	۰	۲	۳	۱۳	۲۲	۲/۹۱۶۶۶۷	۰/۱۶۹۸۶۷
T8	۰	۰	۴	۱۲	۲۴	۳	۰/۰۵۷۶	۰	۰	۲	۱۶	۲۲	۳	۰/۱۷۲۸
T9	۰	۱	۱	۱۳	۲۵	۳/۰۳۳۳۳۳	۰/۰۵۸۲۴	۰	۰	۲	۱۶	۲۲	۳	۰/۱۷۴۷۲
جمع						۲۷/۱۳۳۳۳	۰/۵۲۰۹۶						۲۶/۵۳۳۳۳	۱/۵۳۵۸۸۳
جمع قوت و ضعف						۵۲/۰۸۳۳۳	۱						۴۶/۱۸۳۳۳	۲/۵۸۱۳۲۳

جدول ۱۱: خلاصه ماتریس عوامل خارجی (EFE)

عوامل محیط داخلی	میانگین موافقت	وزن عامل	میانگین وضع موجود (ضریب اهمیت)	نمره موزون
فرصت‌ها	۲۴/۹۵	۰/۴۷۹۰۴	۱۹/۶۵	۱/۰۴۵۴۴
تهدیدها	۲۷/۱۳۳۳۳	۰/۵۲۰۹۶	۲۶/۵۳۳۳۳	۱/۵۳۵۸۸۳
مجموع فرصت‌ها و تهدیدها	۵۲/۰۸۳۳۳	۱	۴۶/۱۸۳۳۳	۲/۵۸۱۳۲۳

بر اساس نتایج حاصله، چون عدد تهدیدات بیشتر از عدد فرصت‌ها می‌باشد بنـابراین جنـگ الکترونیـک نیاجا در محیط خارجی با تهدید روبرو است.

جدول ۱۲: تقسیم‌بندی و تخصیص منابع جنگ الکترونیک نیاجا

عوامل/ درصد منابع تخصیص‌یافته	مقادیر	درصد تخصیص منابع موردنیاز
قــوت‌ها	۰/۳۷۹۶۹	۱۳/۸۳۴۸۴۲۶
ضعف‌ها	۰/۶۲۰۳۱	۳۵/۸۵۳۲۳۶۸۲
فرصت‌ها	۰/۴۷۹۰۴	۲۰/۳۷۶۴۳۳۰۸
تهــدیدها	۰/۵۲۰۹۶	۲۹/۹۳۵۴۸۷۴۹
مجموع قوت‌ها و ضعف‌ها	۲/۵۴۹۳۱۳	۴۹/۶۸۸۰۷۹۴۲
مجموع فرصت‌ها و تهدیدها	۲/۵۸۱۳۲۳	۱۳/۲۴۳۸۰۵۵۸

۴-۳ ماتریس ارزیابی موقعیت و اقدام راهبردی[1] جنگ الکترونیک نیاجا

از ماتریسIFE & EFE جهت تعیین موقعیت راهبردی و تحلیل شکاف به‌صورت ذیل استفاده می‌شود:

مختصات وضع موجود= (A, B)	
نمره موزون ضعف‌ها - نمره موزون قوت‌ها = A	-۱/۱۲۹۶۸
نمره موزون تهدیدات- نمره موزون فرصت‌ها= B	-۰/۴۹۰۴۴۳
C = Arctg A/B	۶۶/۵۳°
زاویه نقطه مطلوب(ایده آل) با محور X ها = D	۴۵°
C+D= مقدار زاویه چرخش راهبردی از وضع موجود به وضع مطلوب = ۶۶/۵۳° +۹۰° +۴۵° = ۲۰۱/۵۳°	

[1] STRATEGIC POSITION AND ACTION EVALUATION MATRIX (SPACE)

میزان زاویه چرخش از وضع موجود به وضع مطلوب ۲۰۱/۵۳° درجه می‌باشد. بنابراین وضع موجود جنگ الکترونیک در ناحیه تدافعی یا انفعالی قرار داشته و تهدید محور و در وضعیت ناپایداری قرار دارد و در مواجهه با تهدیدها آسیب‌پذیر و ازنظر منابع و امکانات تخصصی با مشکل مواجه و تأکید به دستیابی به سامانه‌های نوین جنگ الکترونیک با رویکرد ناهمتراز، میانبر و خلاقانه مدنظر می‌باشد. بنابراین برای رسیدن به وضع مطلوب باید با رویکرد مقتدرانه آموزش، تحقیق، توسعه و تولید سامانه‌های نوین جنگ الکترونیک هوشمند و بومی به رویکرد تهاجمی یا فعال برسیم، به فرصت‌ها توجه بیشتری از قوت‌ها و به نقاط ضعف و قوت داخلی توجه بیشتری شود در این صورت جنگ الکترونیک به وضعیت پایدار و مطلوبی خواهد رسید.

۵. نتیجه‌گیری و پیشنهادها

۵-۱ نتیجه‌گیری

با اولویت‌بندی و تعیین مطلوبیت‌های راهبردی با استفاده از نظر ۱۵ نفر خبره و نرم‌افزار topsis، یافته‌های تحقیق به‌عنوان مناسب‌ترین راهبردهای جنگ الکترونیک در برابر تهدیدات آتی دشمن در افق چشم‌انداز ۱۴۰۴ از بین ۲۰ راهبرد در نهایت ۱۲راهبرد، به ترتیب اولویت جدول ۱۳ احصاء گردید:

جدول ۱۳: اولویت‌بندی و مطلوبیت راهبردهای احصاءشده

اولویت	راهبردها	مطلوبیت راهبردها	راهبردهای احصاء شده
۱	راهبرد۳	۰/۷۳۲۳۴۵	بومی‌سازی سامانه‌های جنگ الکترونیک نپاجا با استفاده از توان و ظرفیت‌های علمی دانشگاه‌های نظامی و غیرنظامی و مراکز تحقیقاتی کشور با قطع وابستگی و رسیدن به خودکفایی و خوداتکایی
۲	راهبرد۱۵	۰/۶۵۲۴۳۵	هوشمندسازی میدان نبرد الکترونیکی با به‌کارگیری حساسه‌های پیشرفته و هوشمند (اطلاعات سیگنالی، تصویری و سنجشی و علائمی و سامانه‌های هشداردهنده راداری، لیزری و مادون‌قرمز) به‌منظور کشف و شناسایی دقیق و آنی تهدیدات طیف الکترومغناطیس
۳	راهبرد۷	۰/۶۴۳۲۳۹	به‌کارگیری فناوری‌های ضدشنود و ضدرهگیری با استفاده از به‌کارگیری فناوری احتمال رهگیری و احتمال آشکارسازی کم راداری و فناوری طیف گسترده، خفیفه‌نگاری و پنهان نگاری ارتباطی نپاجا با هدف مصون‌سازی سامانه‌های راداری و ارتباطی
۴	راهبرد۲	۰/۶۱۲۳۴۵	تشکیل سامانه فرماندهی و کنترل جنگ الکترونیک هوشمند و بومی از طریق هم‌افزایی و یکپارچگی زیرساخت‌های نرم‌افزاری و سخت‌افزاری جنگ الکترونیک با پایش تهدیدات جنگ الکترونیک در سطوح راه‌کنشی، عملیاتی و راهبردی
۵	راهبرد۹	۰/۵۸۵۴۳۲	دورایستاسازی عملیات جنگ الکترونیک از طریق طراحی، ساخت و به‌کارگیری سامانه‌های نوین جنگ الکترونیک هواپایه و زمین‌پایه با هدف افزایش شعاع عملیات جنگ الکترونیک
۶	راهبرد۶	۰/۵۲۳۴۹۸	پنهان‌کار نمودن با به‌کارگیری فناوری‌های حفاظت الکترونیک راداری و ارتباطی با هدف ارتقاء پایداری سامانه‌های راداری و ارتباطی
۷	راهبرد۸	۰/۵۱۹۸۶۵	هم‌افزایی و همگرایی جنگ سایبری، جنگ الکترونیک و اطلاعات سیگنالی (سایبر الکترونیک) از طریق بازطراحی ساختار سازمانی، روال‌ها و رویه‌ها، اجرای رزمایشات مشترک و توسعه زیرساخت‌های میدان نبرد الکترونیکی با هدف برتری عملیاتی و قدرت پاسخگویی بالا در برابر تهدیدات دشمن
۸	راهبرد۱	۰/۴۹۷۶۵۴	ارتقاء آموزش‌های جنگ الکترونیک از طریق مراکز آموزشی در کلیه سطوح افسری و درجه‌داری با هدف نهادینه‌سازی فرهنگ جنگ الکترونیک
۹	راهبرد۱۱	۰/۴۵۸۹۲۳	فلج سازی راه‌کنشی و راهبردی دشمن با طرح‌ریزی و اجرای حملات و فریب الکترونیکی پیشرفته راداری، ارتباطی با هدف افزایش بازدارندگی
۱۰	راهبرد۱۴	۰/۴۳۸۷۵۴	مقاوم‌سازی سامانه‌های جنگ الکترونیک خودی از طریق بومی و هوشمند سازی سامانه‌ها با هدف مصون‌سازی در برابر حملات سلاح‌های لیزری، سلاح‌های پرتوی، بمب‌های الکترومغناطیس، موشک‌های کروز، موشک‌های ضدتشعشعی و حملات الکترونیکی دشمن
۱۱	راهبرد۱۰	۰/۳۹۴۵۸۹	بازطراحی آمایش سامانه‌های جنگ الکترونیک از طریق اجرای مدل‌ها و الگوهای بومی، دانش‌محور و پاسخگو به تهدیدها با هدف افزایش بازدارندگی و ارتقاء پایداری ملی
۱۲	راهبرد۵	۰/۳۰۳۲۴۵	ایمن‌سازی سامانه‌های راداری و ارتباطی نپاجا از طریق طراحی، ساخت و به‌کارگیری سامانه‌های نرم‌افزاری و سخت‌افزاری ضدشنود و ضدرهگیری هوشمند بومی با هدف ارتقاء امنیت پایدار

۵-۲ پیشنهادها

با توجه به عوامل احصاء شده و راهبردهای تدوین‌شده، پیشنهادها اجرایی جنگ الکترونیک ذیل ارائه می‌گردد:

۱. اصلاح ساختار سازمانی جنگ الکترونیک در کلیه سطوح عملیاتی، راه‌کنشی و راهبردی.
۲. آموزش و نهادینه‌سازی الزامات جنگ الکترونیک در کلیه سامانه‌های راداری و ارتباطی.
۳. هم‌افزایی کلیه زیرساخت‌های جنگ الکترونیک در طرح‌های آمایش سرزمینی.
۴. بومی‌سازی و هوشمندسازی کلیه زیرساخت‌های جنگ الکترونیک.
۵. به‌کارگیری فرماندهی و کنترل جنگ الکترونیک هوشمند بومی در نپاجا.
۶. ایمن‌سازی و مقاوم‌سازی جنگ الکترونیک با اجرای اصول و الزامات پدافند غیرعامل.
۷. به‌کارگیری فناوری‌های پیشرفته جنگ الکترونیک در سامانه‌های راداری و ارتباطی.

منابع

[۱] جواهری، علیرضا. (۱۳۹۲). جنگ الکترونیک. انتشارات دانشگاه هوایی شهید ستاری. ص ۱۹۹.

[۲]جواهری، علیرضا. (۱۳۹۲). جنگ الکترونیک. انتشارات دانشگاه هوایی شهید ستاری. ص ۲۰۱.

[3] U.S. HOUSE of REPRESENTATIVES. (2008), p25.

[4] Joint Publication. (2007) "Electronic Warfare", January, p3-31.

[۵] واحدی، مرتضی. قیاسی، علی‌اکبر. (۱۳۹۰). کلیات جنگ الکترونیک. تهران: انتشارات حفاظت اطلاعات آجا. ص ۱۶۳.

[۶] عفیفی، احمد. کریم‌زاده، مرتضی. نظافتی، محمدباقر. (۱۳۸۵). جنگ الکترونیک برای صحنه نبرد دیجیتالی. تهران: موسسه آموزشی تحقیقاتی وزارت دفاع. ص ۲۳۶.

[۷] هندی، امیر. اسکندر زاده، عباس. (۱۳۹۰). فناوری‌های مقابله با بمب‌های الکترومغناطیس. تهران: دانشگاه هوایی شهید ستاری. ص ۱۳۴.

[8] Defense, US Department. (2005). P4.

[9] Joint publication. (2006). Chap 4. p3-13.

[10] AIR FORCE DOCTRINE DOCUMENT. (2002). p5-35.

[۱۱] اسفندیاری، مسعود. سپهری، محمد. (۱۳۸۷). بررسی تطبیقی و پایش تهدیدات فناورانه جنگ الکترونیک و ترازیابی توان فناورانه ایران و آمریکا و ارائه الگوی تحلیلی مناسب. تهران: موسسه آموزشی پژوهشی وزارت دفاع. ص ۱۴۴.

[۱۲] ویتفورد، ری. (۱۳۹۰). روند تکامل طراحی جنگنده‌ها- WWW. nasa. Com. ص ۲۹.

[۱۳] ویتفورد، ری. (۱۳۹۰). روند تکامل طراحی جنگنده‌ها- WWW. nasa. Com. ص ۳۰.

[14] neri, Filippo. (2003). Introduction to Electronic Defense System-Artech House-(SECOND EDITION). P373-519.

[۱۵] دربهانیها، علی.سپهری، محمد. (۱۳۹۰). پرنده‌های هدایت‌پذیر از دور و نزدیک. تهران: انتشارات دانشگاه هوایی شهید ستاری. ص ۴۵.

[16] NICHOLAS M , SHORT SH.RT, MILITARY .(2007) .INTELLIGENCE SATTELITE". P7-12.

[۱۷] سپهری، محمد. (۱۳۹۶). راهبردهای پدافند غیرعامل سامانه‌های راداری و ارتباطی آجا در برابر تهدیدات از منظر حساسه‌های اطلاعات سیگنالی دشمن. دانشگاه عالی دفاع ملی. ص ۱۲۸-۱۹۳.

[۱۸] افشاری، محمد. جواهری، علیرضا. (۱۳۸۸). تحلیل عملیاتی نیروی هوایی تا سال ۲۰۲۵- موسسه آموزشی تحقیقاتی وزارت دفاع. ص ۱۴۶.

[۱۹] رزم‌خواه، محمدرضا. (۱۳۸۷). بررسی تطبیقی پایش تهدیدات فناورانه اطلاعاتی و ترازیابی توان فناورانه ایران و آمریکا و ارائه الگوی تحلیلی مناسب. تهران: موسسه آموزشی پژوهشی وزارت دفاع. ص ۵۵.

[۲۰] جلالی، غلامرضا. (۱۳۹۱). چهار گفتار در باب پدافند غیرعامل تهران: انتشارات محدث. ص ۱۲۳.

[۲۱] اسفندیاری، مسعود. سپهری، محمد. (۱۳۸۷). بررسي تطبيقي و پايش تهديدات فناوري‌هاي جنگ الكترونيک هوايي و ترازيابي توان فناوري‌هاي جنگ الكترونيك هوايي دو كشور ايران و آمريكا و ارائه‌ی الگوي تحليلي مناسب و استخراج فناوري‌ها و تجهيزات جنگ الكترونيک هوايي ايران و مستندسازي آن‌ها، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی. ص۶۵.

[۲۲] رزم‌خواه:، محمدرضا. (۱۳۹۰). نقش حساسه‌های جمع‌آوری اطلاعات در دفاع غیرعامل. بوستان حمید. ص ۷۷.

[۲۳] رزم‌خواه، محمدرضا. (۱۳۸۷). بررسی تطبیقی پایش تهدیدات فناورانه اطلاعاتی و ترازیابی توان فناورانه ایران و آمریکا و ارائه الگوی تحلیلی مناسب. تهران: موسسه آموزشی پژوهشی وزارت دفاع. ص ۶۲- ۲۷۵.

[۲۴] عرفانی، اسماعیل. حسینی، سید احمد. سعیدآوی، جبار. (۱۳۹۲). جمع‌آوری، تجزیه‌وتحلیل و پردازش اطلاعات سامانه‌های جنگ الکترونیک ارتش آمریکا مستقر در خلیج‌فارس.تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی. ص ۲۴۰-۲۷۵.