فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دوم، شماره ۱، بهار ۱۳۹۷

# مدل ارزیابی آسیب‌پذیری‌های عملیات شبکه محور مبتنی بر فرایند تحلیل سلسله‌مراتبی

مهدی ملازاده گل محله [۱]، حمیدرضا لشکریان [۲]، مجید شیخ‌محمدی [۳]، کمال میرزائی [٤]

تاریخ دریافت: ۱۳۹٦/۰۷/۱۹ تاریخ پذیرش: ۱۳۹۷/۰۳/۲۵


## چکیده

پیش‌بینی نبردهای آینده، موضوعی است که چند دهه بین نظریه‌پردازان موردبحث است. به اعتقاد آن‌ها صحنه نبرد چنین جنگی شبکه محور، پیچیده، غیرخطی، پویا و در فضای عدم قطعیت انجام خواهد شد این در حالی است که بر مبنای تئوری پیچیدگی و آشوب مشکلات و آسیب‌های جزئی می‌تواند اثرات و پیامدهای مخربی در این محیط پیچیده داشته باشد بنابراین ارزیابی آسیب‌های آن از ضروریات تحقیق است. این تحقیق ازنظر هدف کاربردی است. شیوه تحقیق بر اساس تجزیه وتحلیل اسناد و مطالعه کتابخانه‌ای جهت استخراج آسیب‌ها و معیارهای ارزیابی انجام‌شده است. سپس با ارائه الگویی بر مبنای فرایند تحلیل سلسله مراتبی به ارزیابی و رتبه‌بندی آسیب‌های عملیات شبکه محور پرداخته است. در این مقاله معیارهای؛ زمان، هزینه، اثربخشی و امکان‌پذیری، برای ارزیابی آسیب‌پذیری‌ها جهت استفاده مؤثر تعیین‌شده است. با در نظر گرفتن معیارهای ارزیابی، آسیب‌پذیری‌های جنگ الکترونیک، فنّاوری و فرماندهی بیشترین اولویت جهت استفاده می‌باشند. از منظر زمان، آسیب‌پذیری‌هایی چون جنگ الکترونیک، فنّاوری و نیروی انسانی دارای بالاترین رتبه‌بندی جهت استفاده می‌باشند. از منظر هزینه استفاده از آسیب‌پذیری‌هایی چون شبکه و ارتباطات، فنّاوری و جنگ الکترونیک دارای بالاترین اولویت و آسیب‌پذیری‌های فرماندهی مانند فرسایشی نمودن جنگ و افزایش بار اطلاعاتی کمترین رتبه‌بندی هزینه را به خود اختصاص داده است. اثرگذارترین آسیب‌پذیری پیشرفت علوم شامل تئوری‌های پیچیدگی، آشوب و تئوری سیستم است. کم اثرترین آسیب‌پذیری در عملیات شبکه محور آسیب‌های ارائه شده ناشی از فنّاوری است. ازلحاظ امکان‌پذیری نیز آسیب‌های فرماندهی، خطرات اطلاعاتی بیشترین رتبه‌بندی را به خود اختصاص دادند که با عملیات روانی و شناختی و با هزینه بالا قابل حصول است و خطرات ناشی از فریب اطلاعاتی و پیشرفت علوم کمترین رتبه را به خود اختصاص دادند.


**کلمات کلیدی**: **آسیب‌پذیری، تصمیم‌گیری چندمعیاره، فرایند تحلیل سلسله مراتبی، عملیات شبکه محور**

[۱] دانشجوی دکتری دانشگاه جامع امام حسین (ع)، mmollazadeh@ihu.ac.ir

[۲] استادیار، عضو هیات علمی دانشگاه جامع امام حسین (ع)

[۳] استادیار، عضو هیات علمی دانشگاه تربیت مدرس، msheikhm@modares.ac.ir

[٤] استادیار، عضو هیات علمی دانشگاه آزاد اسلامی، میبد یزد، k.mirzaie@maybodiau.ac.ir

## ۱. کلیات

پای نهادن به عصر اطلاعات تحولاتی ژرف را در تمامی زمینه‌های زندگی انسانی پدید آورده است. این تغییرات ریشه چالش‌هایی گسترده برای سازمان‌های نظامی خواهد شد. در عصر اطلاعات رمزِ بقا و شرط تداوم هر سازمانی تجهیز به سلاحی با مزیت رقابتی است. عصر اطلاعات شرایطی را به سازمان‌ها تحمیل می‌کند که بر اساس آن باید ساختار، هزینه‌ها، روش‌ها و فرایندهای خود را تغییر دهند. پیروزی متعلق به آنانی است که به اهمیت و قدرت " اطلاعات" و فناوری‌های مرتبط به آن پی‌ببرند و با توجه به آن مزایای رقابتی خود را گسترش دهند. سازمانی در فضای رقابتی قوی‌تر است که از برتری اطلاعاتی[۵] بیشتری بهره‌مند باشد. همچنین در عصر اطلاعات گستره میدان نبرد به‌طور قابل‌توجهی وسیع‌تر و آهنگِ اجرایی عملیات سرعت بیشتری خواهد داشت و اصل غافلگیری به محوری‌ترین اصل نبرد تبدیل خواهد شد که این امر از تفوق و برتری اطلاعاتی نشأت می‌گیرد.

### ۱-۱. بیان مسئله

در سند چشم‌انداز مشترک آمریکا و همچنین سند چشم‌انداز نیروی‌های مسلح آمریکا، شدیداً وابسته به این مفهوم می‌باشند که به‌طور بالقوه پیوند دادن یگان‌های رزمی که ازلحاظ جغرافیایی پراکنده می‌باشند از طریق شبکه‌سازی صورت می‌پذیرد؛ بنابراین انتظار نیروی مسلح آمریکا بهبودی و توسعه مناسب از فهم فضای نبرد مشترک و افزایش اثربخشی درگیری و نبرد از طریق اقدامات هماهنگ و هم‌زمان است. دفتر تحول نیروی[۶] آمریکا برای محقق نمودن اهداف سند چشم‌انداز، ساختار نیرویی اساساً مشترک، شبکه محور و توزیع‌شده با برتری تصمیم‌گیری سریع را ارائه نموده است. دفتر تحول این مفهوم مشترک عملیاتی جدید را در قالب مفهوم جنگ شبکه محور[۷] ارائه نموده است. جنگ شبکه محور به‌عنوان نماد جنگ در عصر اطلاعات ارائه‌شده است [۱]. جنگ شبکه محور بر این نکته تأکید دارد که با ارتباط و شبکه‌بندی مؤثر بین مؤلفه‌ها جهت تبادل اطلاعات، قدرت نظامی افزایش می‌یابد. البته شبکه‌بندی در جنگ شبکه محور، تنها به معنی اتصال فیزیکی مؤلفه‌ها نیست بلکه به فرایندهایی که موجب هم‌افزایی می‌شود تأکید دارد.

### ۲-۱. اهمیت ضرورت و موضوع تحقیق

در عصر جدید، نقشه‌راهی که آمریکا را به سمت یک نیروی آیندهِ مطلوب سوق می‌دهد دگرسازی و تغییر در نیروی نظامی است. نیروی مشترک آمریکا در محیطی عملیات خواهد نمود که پیچیده و پویاست. دیگر قوانین خطی در این محیط کارا نمی‌باشد[۸]. از نگاه آمریکا و متحدانش اگر آمریکا در دگرسازی و تحول نیروی نظامی جدید متحمل شکست شود، برتری فعلی به‌شدت با چالش روبرو خواهد شد. رقیب‌های منطقه‌ای ایجاد خواهد شد، تعارضات بسیار محتمل خواهد شد [۱]. از منظر اسناد غربی، وزارت دفاع آمریکا می‌بایست به

[5] Information Superiority
[۶] Office of Force Transformation (OFT)
[۷] Network Centric Warfare (NCW)

[۸] اندرو و ایلاچینسکی نخستین بار در پروژه آلبرت در سال ۱۹۹۶ میلادی، صحنه نبرد را به‌عنوان سیستم انطباقی پیچیده مطرح نمودند که از تعداد زیادی عناصر وابسته تشکیل شدند و دیگر روابط خطی مانند معادلات لانچسترکه برای مدل‌سازی صحنه نبرد استفاده می‌شد، کارایی نداشت

سمت بدست آوردن ساختار نیرویی اساساً مشترک، شبکه محور و توزیع‌شده تغییر نماید تا قادر به داشتن برتری سریع تصمیم‌گیری باشد. برای رسیدن به این هدف، وزارت دفاع آمریکا در حال بنا نمودن دکترین، آموزش، آماد و تمرینات، برای ایجاد یک فرهنگ مداوم دگرسازی است که شامل افراد، فرآیند و سیستم‌ها است. پس‌نیاز است که این تحولات رصد، مطالعه، تحلیل قرارگرفته و آسیب‌پذیری‌ها و نقاط قوت آن برای مقابله جدی استخراج شود.

بعد از ارائه مفهوم جنگ شبکه محور تلاش‌های بسیار زیادی برای بررسی چالش‌های پیاده‌سازی آن شده است. وزارت دفاع آمریکا برای اثبات مزیت‌های عملیات/جنگ شبکه محور[۹] مانورهای نظامی زیادی را انجام داده است. آمریکا پس از اطمینان از اثربخشی مفهوم جنگ شبکه محور در سال ۲۰۰۳ در بخش‌هایی از نبرد با عراق از این دکترین استفاده کرده است همچنین در جنگ‌های نامنظم در افغانستان در سال ۲۰۰۹– ۲۰۱۱ برای مبارزه با گروه طالبان گزارش‌شده است [۱]. همچنین با توجه به رویکرد اکثر کشورهای غربی و اخیراً آسیایی به سمت شبکه محوری[٤][۳] [۲]، دغدغه آن‌ها نسبت به آسیب‌پذیر بودن چنین دکترین نظامی بسیار زیاد است. دیدگاه آن‌ها این است که دشمنان و مخالفان آن‌ها در حال رصد مداوم فعالیت‌های آن‌ها می‌باشند و ضعف‌هایی که از مفاهیم جدید نظامی استخراج می‌شود را منتشر نمی‌کنند به‌طوری‌که صحبت‌های میلان وگو[۱۰] در این مورد قابل تأمل است [۵]:

«جنگ شبکه محور به‌سرعت به یک ارتودوکسی تبدیل‌شده است (یکسری از اعتقاداتی که به‌طور جدی مورد چالش و بررسی واقع نشده است) معایب و آسیب‌های جدی آن به صورت عمومی منتشر و مورد بحث واقع نشده است و یا با اکراه پذیرفته شده است.... دشمن به‌ندرت چیزی در مورد آسیب‌ها ذکر کرده باشد و چنین به نظر می‌رسد که دشمن از خنثی کردن طرح و فعالیت‌های ما ناتوان است.» همچنین در منابعِ نقد آن‌ها همیشه سخنان وانگ پوفنگ[۱۱] ژنرال ارتش سرخ چین و برجسته است که می‌گوید: «ما بایستی از انواع، شکل‌ها و روش‌های نیروی نظامی و مخصوصاً استفاده از جنگ‌های غیرخطی و روش‌های متعدد جنگ اطلاعات که ترکیبی از عناصر غربی و بومی هستند را برای استفاده از توانمندی‌هایمان جهت حمله به ضعف‌های دشمن، جلوگیری از واکنش آن‌ها و تلاش و کوشش برای مؤثر واقع شدنمان انجام دهیم. با این رویکرد برای چین به دست آوردن یک پیروزی فراگیر بر دشمن حتی در شرایط پست و مادونی[۱۲] فنّاوری اطلاعاتی، کاملاً امکان خواهد داشت» [۷].

حساسیت بسیار زیاد آسیب‌پذیری‌های جنگ شبکه محور به دلیل محیط پیچیده جنگ و رفتار آشوبناکی آن است که آسیب‌های ناچیز با توجه به اصل پروانه‌ای[۱۳] می‌تواند منتج به نتایج و تأثیرات بسیار وسیع و بزرگ شود. این اصل حتی ضرورت و بررسی آسیب‌هایی که در نگاه اولیه کم‌تاثیر و کم‌مخاطره به نظر می‌رسد را بسیار جدی‌تر نموده است. به همین دلیل تحلیل‌گران

[۹] این دو عبارت در بسیاری از منابع به‌جای هم استفاده می‌شود

[۱۰] Millan Vego

[۱۱] Wang Pufeng

[۱۲] Inferiority

[۱۳] Butterfly

نظامی در این محیط جدید حتی آسیب‌هایی با مخاطره کم را با جدیت موردبررسی قرار می‌دهند [۱]. با توجه به احتمال رویارویی ج.ا.ا با آمریکا در یک عملیات شبکه محور، بررسی و ارزیابی آسیب‌ها و نحوه استفاده و مدیریت این آسیب‌ها با توجه به پیچیدگی مسئله برای ج.ا.ا از اهمیت بالایی برخوردار است. در این راستا ضرورت معیارهای ارزیابی آسیب‌پذیری‌ها، تحلیل و ارزیابی آسیب‌ها بر اساس هریک از معیارها لازم و ضروی به نظر می‌رسد تا بتوان بر مبنای تحلیل درست و ارزیابی دقیق تصمیم‌های ضروری را در زمان مناسب اتخاذ شود.

### ۱-۳. پرسش تحقیق

با توجه ضرورت ارزیابی آسیب‌پذیری‌های عملیات شبکه محور، پرسش اصلی این پژوهش عبارت است از:

۱- مدل ارزیابی آسیب‌پذیری جنگ شبکه محور بر اساس فرایند تحلیل سلسه مراتبی چگونه است؟

برای پاسخگویی به این سؤال اصلی نیاز به جواب به سؤالات فرعی زیر است:

۱- دسته‌بندی مناسب این آسیب‌پذیری چگونه است؟
۲- معیارهای اساسی برای ارزیابی آسیب‌شناسی جهت بهره‌مندی مناسب از آن چیست؟
۳- ارزیابی و رتبه‌بندی آسیب‌ها بر مبنای معیارها چگونه است؟

### ۱-٤. هدف تحقیق

هدف اصلی این تحقیق ارائه مدلی برای ارزیابی و اولویت‌بندی آسیب‌پذیری‌های جنگ شبکه محور است. برای رسیدن این هدف، دسته‌بندی مناسب آسیب‌پذیری‌ها و استخراج معیارهای ارزیابی آسیب‌پذیری نیز در راستای اهداف اصلی این پژوهش است.

### ۱-۵. پیشینه تحقیق

با بررسی منابع آشکار در داخل کشور سندی مبنی بر بررسی و ارزیابی آسیب‌پذیری‌های جنگ شبکه محور به دست نیامده است عمده فعالیت در این حوزه بررسی مفاهیم مرتبط با جنگ شبکه محور و یا مدل‌سازی صحنه شبکه محور با رویکردهای خاص بوده است که بعضی از سندهای مهم عبارت‌اند از؛ [۱۲] [۱۳] [۱٤] [۱۵].

در این تحقیق با بررسی مقالات در منابع آشکار، آسیب‌پذیری‌ها به جنگ شبکه محور به‌صورت زیر دسته‌بندی‌شده است؛

#### ۱-۵-۱. از منظر پیشرفت علوم

پیشرفت‌های علوم مانند تئوری سیستم‌ها و علوم پیچیدگی سعی در مدل‌سازی یک سیستم پیچیده می‌باشند. این آسیب‌پذیری‌ها از چالش‌های جدی و ذاتی عملیات شبکه محور است. همچنین در یک بازه‌ی زمانی محدودی دکترین جنگ شبکه محور با نگاه فلسفی دقیق مورد تحلیل و ارزیابی قرار گرفته است.

#### ۱-۱-۵-۱. آسیب‌پذیری از منظر علوم پیچیدگی

مخاطرات و آسیب‌های ارائه شده از منظر رفتار انطباقی پیچیده[۱٤]، تناقض بین ویژگی خودهمزمان‌سازی و خودسازمان‌دهی و اثرات شبکه بوده است. ویژگی تغییراتِ رفتاری در این‌گونه سیستم‌ها، می‌تواند غیرقابل پیش‌بینی و از تغییرات نسبتاً کوچک در مقیاس بسیار بزرگی که همان رفتار آشوبی (اصل پروانه‌ای) است، ایجاد شود. [۱٦]. با بررسی دقیق منابع [۱۷] و [۱۸] می‌توان نتیجه گرفت این آسیب‌پذیری از ذاتِ اصلی یک سیستم پیچیده منتج می‌شود. ساختار ارتش آمریکا به دلیل بهره‌مندی از مزایای شبکه محوری و برای جلوگیری از چنین ضعفی درصدد مدیریت مخاطرات آن است [۱۹].

[۱۴] Complex Adaptive Behaviour

تضاد بین ویژگی خودسازمان‌دهی در سیستم پیچیده با ویژگی خود هماهنگی در انگاره‌های جنگ شبکه محور نیز از آسیب‌پذیری‌های دیگر است. همچنین بیان شده که برخلاف قاعده مت‌کالف[۱۵] افزایش کاربران جدید، منابع و ذخایر داده، باعث افزایش ارزش یک شبکه نخواهد شد و شاید منجر به کاهش بازدهی و ارزش یک شبکه شود [۱٦].

**۲-۱-۵-۱. از منظر علوم فلسفه**

رویکرد دیگر ارزیابی از نگاه مفهوم‌شناسی است که توسط آقای گیفین ارائه‌شده است [۲۰]. ایشان بحثی با عنوان روش علمی بی‌اعتباری[۱٦] ارائه نمودند که با عنوان «استقراگرایی»[۱۷] بیان‌شده است. گیفین به‌صورت مباحثه ادعا نموده است که بسیاری از اصول و قواعدی جنگ شبکه محور بر مبنای یک فلسفه ضعیف و اشتباه[۱۸] ارائه‌شده است. بر اساس فعالیت‌های دو فیلسوف به نام‌های هیوم و پوپر[۱۹]، مراحل روش بی‌اعتباری برای جنگ شبکه محور به‌صورت قدم‌به‌قدم مورد تحلیل و ارزیابی قرار گرفت و نشان داده شد که آن‌ها اساس و مبنای علمی دقیقی ندارند. آقای گیفین این بحث را مطرح نموده که نه‌تنها بسیاری از اصول و قواعدی مطرح شده، بلکه تمام مفاهیم ارائه شده در تحول امور نظامی[۲۰] بر مبنای این روش، معیوب است. مقاله انتقادی دیگری در همین راستا در دو بخش کلی ارائه‌شده است [۲۱]:

بخش اول: جنگ شبکه محور بر اساس یک جمع‌آوری از اجزای ساده که مجموعه‌ای از تمثیل‌های کسب‌وکار است، شکل‌گرفته است و این نکته‌ای بوده که توسط کافمن[۲۱] نیز ارائه‌شده است [۲۲].

بخش دوم: مسائل مربوط به روش بی‌اعتباری است.

آقای گیفین در گام بعد ادعا نموده است که به دنبال تعریف یک چارچوب مفهومی جدید بر اساس علوم درست و دقیق خواهد بود اما از آن زمان تاکنون هیچ مطلبی و سندی دال بر ادامه این پژوهش در منابع آشکار وجود ندارد.

**۲-۵-۱. آسیب‌پذیری از منظر فنّاوری**

**۱-۲-۵-۱. آسیب‌پذیری از منظر شکاف فنّاوری**

بارنِت[۲۲] از موسسه نیروی دریایی آمریکا [۲۳] و بورگ در اجلاس ۲۰۰۳ [۲٤] شکاف فنّاوری بین نیروها و در سطحی بالاتر بین نیروهای هم‌پیمانان آمریکا و ناتو را به عنوان آسیب جدی ارائه نمود. پس از ارائه این آسیب، آمریکا و هم‌پیمانان با همکاری شرکت‌های نظامی/غیرنظامی پیشرو در فنّاوری و با ایجاد کنسرسیومی[۲۳] در حال ایجادِ تعامل و همکاری بین سامانه‌های مختلف اعضا، جهت همکاری و هماهنگی محصولات خود در عملیات شبکه محور می‌باشند.

**۲-۲-۵-۱. آسیب‌پذیری از لحاظ محدودیت‌های فنّاوری**

یکی دیگر از چالش‌های فنّاوری دررسیدن به بلوغ شبکه محوری میزان پهنای باند مورد نیاز برای انتقال اطلاعات است. مطابق جدول (۱) با مقایسه افزایش روبه رشد پهنای باند در جنگ‌های اخیر برای انتقال اطلاعات، این مسئله برجسته شده است [۲۵].

**جدول ۱: میزان استفاده از پهنای باند در جنگ‌های اخیر [۲۵]**

| شماره | عنوان درگیری | پهنای باند مورد استفاده |
|---|---|---|
| ۱ | طوفان صحرا ۱۹۹۱ | 99 Mbps |
| ۲ | کوزوو ۱۹۹۰ | 250 Mbps |
| ۳ | نبرد آزادی ۲۰۰۲ | 736 Mbps |
| ٤ | آزادی عراق ۲۰۰۳ | 3200 Mbps |

[۱۵] Met' Calf
[۱٦] Discredited Scientific Method
[۱۷] Inductivism
[۱۸] Flaw
[۱۹] Hume and Popper
[۲۰] Revolution in Military Affairs (RMA)
[۲۱] Kaufman
[۲۲] Barnett
[۲۳] Network Centric Operations Industry Consortium

**۳-۲-۵-۱. آسیب‌پذیری از لحاظ عدم تقارن فنّاوری**

مسئله انتقال فنّاوری در حوزه نرم‌افزار و سخت‌افزار و رسوب دانش آن در کشورهای دیگر از آسیب‌های جدی ذکر شده است [۲۵]؛ به عبارت دیگر آمریکا نمی‌تواند از جنگ شبکه محوری که به عنوان عدم تقارن فنّاوری خود با سایرین ذکر نموده است اتکای بیش‌ازحد کند. محققان هندی این مسئله را در حوزه نرم‌افزار مورد توجه خاص قرار داده‌اند. این محدودیت در سال ۲۰۱٤ برای نیروی شبکه محور آمریکا نیز برجسته شده است [۲٦].

**٤-۲-۵-۱. افزایش خطرات ناشی از استفاده از فنّاوری تجاری**

بودجه‌های نظامی در حال کاهش است و بخش تجاری مسئول بیشتر پیشرفت‌های فنی است. نتیجه آن است که نیروهای نظامی برای پشتیبانی از نیروها، خود را با فنّاوری غیرنظامی تطبیق دهد. درنتیجه باعث وابستگی به فراهم‌کنندگان خدمات تجاری می‌شود. نهایتاً سیستم‌های نظامی آسیب‌هایی مشابه سیستم‌های غیرنظامی خواهند داشت [۲۷] [۲۸].

**۳-۵-۱. آسیب‌پذیری از منظر شبکه**

**۱-۳-۵-۱. آسیب‌پذیری از منظر تقویت درون‌گرایی در شبکه**

به دست آوردن اشراف اطلاعاتی ممکن است ارتباطات گسترده را کم‌رنگ و غیرفعال کند. تئوری‌های جنگ شبکه محور بر تقویت شبکه داخلی جهت رسیدن به اشراف اطلاعاتی تأکید دارد درنتیجه با محدودیت ارتباطات گسترده بیرون شبکه و محدود شدن توانایی روبرو خواهیم شد. پس می‌بایست تعریف درستِ عملیاتی از اشراف اطلاعاتی ارائه شود و نباید به بهانه اشراف اطلاعات زیرساخت‌های اطلاعاتی دشمن را از کار بی اندازیم. چون برای نیروهای خودی به دست آوردن اطلاعات در مورد قصد و نیت و فعالیت‌های دشمن سخت‌تر خواهد شد. در این اسناد مفهوم واقعی اشراف اطلاعاتی بر دشمن به معنی کنترل بهتر بر فضای جنگ و اطلاعات اشتراکی، بیان شده است [۲۳] [۲۹].

رویکرد دیگر آن است که خود هماهنگی یا خودهمزمانی ممکن است قابلیت یک ارتباط و تعامل مؤثر خارجی را از بین ببرد خودهمزمانی اقدامی جهت بالا بردن سرعت عملیات یا چالاکی و انطباق‌پذیری است. بدین منظور تأکید بر روی هماهنگی درون سیستمی یا درون‌سازمانی است؛ اما در نبردهایی که احتمالاً در آینده پیش‌بینی می‌شود نیاز به راهکار بهتری برای تصمیم‌گیری و انجام عملیات است و استفاده از خودهمزمانی نمی‌تواند راهکار مناسبی باشد [۲۹].

**۲-۳-۵-۱. آسیب‌پذیری از نبود یک شبکه جامع و مرجع**

لیتوتیس، آسیب‌پذیری جنگ شبکه محور را در محیط ائتلافی مورد بررسی قرار داده و اولین آسیب جدی را از منظر شبکه بیان نموده است. اینکه تاکنون فعالیتی برای طراحی و ارائه یک شبکه استاندارد برای نیروهای ائتلاف و همکار آمریکا دیده نشده است به‌طوری‌که در جنگ‌های اخیر مثل عراق و افغانستان بیش از ۸۰ نوع شبکه مختلف ارائه و مورد استفاده قرار گرفت. سپس قابلیت همکاری اعضا در شبکه[۲٤] و دسترسی، مدیریت شبکه، مدیریت اطلاعات، محافظت و ساختار شبکه و ارتباطات، محدودیت پهنای باند و دسترس‌پذیری را ذکر نمود [۳۰]. این آسیب‌پذیری نیز توسط محققان دیگری نیز بیان شده بود [۲٦].

[۲۴] Interoperability

**۳-۳-۵-۱. آسیب‌پذیری از منظر شبکه‌های ارتباطاتی**

مرجع [۲۵] امنیت و سطوح امنیتی مختلف در شبکه‌های ارتباطاتی را به‌عنوان چالش‌های بسیار مهم ارائه نموده است و به‌طور مشخص ماهواره‌ها به‌عنوان شبکه‌های ارتباطی از چالش‌های مهم ارتباط دانست. به‌طوری که ۸٤٪ از پهنای باند مورد استفاده ماهواره‌های ارتباطی از ماهواره‌های تجاری است که بسیار آسیب‌پذیر می‌باشد. این آسیب‌پذیری توسط [۱۹] در یک گزارش دانشگاهی مورد بررسی قرارگرفته است.

**٤-۵-۱. آسیب‌پذیری از منظر نیروی انسانی**

**۱-٤-۵-۱. کم‌رنگ شدن نقش نظارتی نیروی انسانی**

کم‌رنگ شدن نقش نظارتی نیروی انسانی مانند تخصیص سطح اتوماسیون؛ تصمیم‌گیری توزیع‌شده و هماهنگی تیم‌ها؛ نقش نیروی انسانی برای ارائه راهکارهای اصلی کاهش پیچیدگی؛ تخصیص اخطار و توجه؛ مانیتورینگ نظارتی اپراتورها؛ اعتماد و قابلیت اطمینان؛... را ذکر نمود [۳۱]. این آسیب‌ها می‌تواند باعث کاهش اثربخشی یک نیروی شبکه محور گردد.

**۲-٤-۵-۱. پراکندگی و فنّاوری منجر به کاهش روابط اجتماعی می‌شود**

جنگ شبکه محور از مفهوم پراکندگی نیروها پشتیبانی می‌کند تا سرعت را افزایش و آسیب‌پذیری را کاهش دهد؛ اما این رویکرد، پیوستگی و باهم بودن نیروها را به چالش می‌کشاند درحالی‌که آن‌ها در آموزش‌ها و جنگ‌ها همواره باهم بوده‌اند. این مسئله ممکن است موجب کاهش اعتمادبه‌نفس نیروها شود [۳۲]. در [۳۰] کاهش روابط اجتماعی و فرهنگی در نیروی ائتلاف و هم‌پیمانان به عنوان آسیب جدی برجسته شده است.

**۳-٤-۵-۱. تشکیل سریع گروهای مأموریتی باعث آسیب‌پذیری تعامل‌های اجتماعی می‌شود.**

تشکیل سریع گروه‌های عملیاتی این عیب را دارد که قبل از مؤثر بودن گروه، زمان زیادی برای پیوستگی اجتماعی افراد گروه نیاز است. این فرایند هر بار که نیاز به تشکیل سریع گروه باشد تکرار می‌شود. این مسئله موجب تضعیف سرعت عملیات، کاهش اعتماد و همکاری غیر مؤثر می‌شود [۳۲].

**٤-٤-۵-۱. فرسایشی شدن جنگ شبکه محور و کاهش اثربخشی نیرو**

یکی از چالش‌های جدی جنگ شبکه محور فرسایشی شدن سامانه‌ها و نیروی انسانی است. اگر زمان درگیری و نبرد در این محیط پیچیده طولانی شود، کارایی و اثربخشی نیرو و فرماندهی و کنترل خیلی سریع کاهش خواهد یافت [۳۳].

**۵-۵-۱. افزایش آسیب‌پذیری از محیط اطلاعاتی جدید و فشار برای پاسخ‌دهی سریع**

**۱-۵-۵-۱. افزایش سرعت منجر به پاسخ‌دهی نامناسب خواهد شد**

یکی از مزایا حرکت به سمت شبکه محوری افزایش سرعت پاسخ‌دهی به وقایع و پیشامدها در چرخه تصمیم‌گیری نیروی نظامی آمریکا است. بالا رفتن سرعت در بستر شبکه محوری، موجب افزایش اطلاعات جمع‌آوری شده از دشمن خواهد شد و عکس‌العمل مناسب اتفاقات را تحت تأثیر قرار می‌دهد. در این حالت باید خیلی سریع به وقایع پاسخ دهیم. معماری شبکه در خصوص سرعت پردازش و توزیع داده، دارای مزیت است اما این مزیت ممکن است به‌درستی مورد بهره‌برداری قرار نگرفته باشد و منجر به افزایشِ سرعتِ

واکنشِ نامناسب گردد. پس آسیب‌پذیری در آن است که بخواهیم فریب قابلیت شبکه که اجازه انجام سریع کارها را می‌دهد، داشته باشیم [۲۳] [۳٤].

**۲-۵-۵-۱. افزایش بار اطلاعاتی و سرعت همراه با افزایش کشندگی، یک ترکیب خطرناک است**

فنّاوری به‌صورت بالقوه باعث پیچیدگی صحنه نبرد می‌شود و همچنین انجام وظائف برای تیم فرماندهی بسیار سخت‌تر می‌شود. جنگ شبکه محور درجه بیشتری از اطلاعات را نه از لحاظ مقدار بلکه ازلحاظ محتوی در اختیار تیم فرماندهی و تصمیم‌گیران قرار می‌دهد؛ بنابراین به فهم و درک بیشتری از محتوی نیاز است. همچنین با توجه به قابلیت‌های شبکه، ارائه اطلاعات بسیار انبوه بدون فهم محتوی، بسیار زیاد است.

پس برای فرماندهان بار اطلاعاتی در حال افزایش، تجهیزات و جنگ‌افزارهای نظامی با توجه به پیشرفت فنّاوری پیچیده‌تر و امکان انجام حملات سریع‌تر و مخرب‌تر حاصل شده است. این دو فاکتور موجب بالا رفتن اطلاعات دریافتی توسط فرمانده شده و فرصت‌های بیشتری برای انجام عملیات مخرب در زمان کوتاه‌تر را فراهم می‌آورد؛ اما فرماندهان تحت فشار فزاینده رسانه‌ای و سیاسی برای تصمیم‌گیری هستند که گاهی منجر به نتایج نامطلوب خواهد داشت [۳۵] [۳٦].

**۳-۵-۵-۱. افزایش عدم قطعیت و کاهش زمان برای پاسخ‌دهی عوامل مختلفی وجود دارد که موجب بالا رفتن عدم قطعیت نزد فرمانده‌های نظامی می‌شوند. اولاً فرماندهان نباید فقط به فکر نیروهای خودی باشند بلکه اقدامات نیروهای دوست را باید هم در نظر بگیرند. ثانیاً با پیچیده شدن تجهیزات نظامی تردید در مورد نحوه عملکرد آن‌ها بیشتر می‌شود.**

**همچنین فناوری، دکترین‌ها و تاکتیک‌های مختلف باعث بالا رفتن سرعت عملیات می‌شوند از طرفی عدم قطعیت نیز افزایش می‌یابد، همچنین زمان دسترسی برای حذف این عدم قطعیت کاهش یافته است. پس پیچیده شدن تجهیزات نظامی باعث افزایش عدم قطعیت شده، همچنین زمان پاسخ‌گویی به اتفاقات نیز کاهش یافته است [۳٤].**

**٦-۵-۱. آسیب‌پذیری از منظر پردازش اطلاعات**

**۱-٦-۵-۱. تصویر عملیاتی مشترک[۲۵]؛ تخریب و فقدان نمایش واقعیت علیرغم اینکه مفهوم تصویر عملیاتی مشترک عموماً یک مفهوم پذیرفته شده است اما مطالعات گذشته، حاکی از برخی اثرات منفی آن است. این اثرات شامل اضافه بار اطلاعاتی و اعتماد بیش از حد به یک تصویرِ خلاصه‌شده اشتباه است که نه به‌درستی به اشتراک گذاشته شده و نه به‌طور کامل نشان‌دهنده واقعیت است [۱۷].**

**۲-٦-۵-۱. مدیریت اطلاعات منجر به عدم قطعیت برای فرماندهی خواهد شد.**

توانایی‌های اطلاعاتی که توسط جنگ شبکه محور ارائه می‌شوند ممکن است مصرف‌کنندگان را با هجوم اطلاعات مواجه کند. راه‌حل، استفاده از مدیریت اطلاعات به‌صورت هم‌زمان است؛ اما مدیریت اطلاعات به‌تنهایی یک راه‌حل نیست زیرا فناوری و فرایندهای آن به مانند استفاده از فیلترهای اطلاعاتی،... می‌تواند عدم قطعیت‌های جدیدتری را ایجاد کند [۳۷] [۲۹] [۳٦].

**۳-٦-۵-۱. اتکای بیش از حد به زیرساخت‌های اطلاعاتی ونبود توانایی لازم جهت حالت‌های جایگزین**

نیروهای نظامی عادی، از مفاهیم نظامی برای مقابله با مشکلاتی که از ارتباط ضعیف ایجاد می‌شود مانند فرماندهی مأموریت[۲٦] استفاده می‌کنند؛ اما برای یک نیروی شبکه شده که توان آن وابسته به ارتباط است، از

[۲۵] Common Operating Picture(COP)

[۲٦] Mission Command

دست رفتن این ارتباط به مانند یک فاجعه است؛ بنابراین در جنگ شبکه محور بسیار به زیرساخت‌های ارتباطی وابسته است که نقطه مهمی برای بهره‌برداری توسط دشمن است. این ضعف در صورت عدم وجود راه‌حل‌ها و روش‌های جایگزین بسیار خطرناک‌تر نیز خواهد شد [۳۸] [۳۹] [۲۷].

**۷-۵-۱. آسیب‌پذیری از منظر فریب اطلاعاتی**

این آسیب‌پذیری‌ها جزء دسته عملیات اطلاعاتی با تمرکز بر فریب اطلاعاتی می‌باشد که مصادیق آن به صورت زیر می‌باشد؛

**۱-۷-۵-۱. افزایش خطرپذیری ناشی از فریب اطلاعاتی**

استراتژی‌های مختلفی نظیر حمله به شبکه جهت ایجاد اشکالات تصادفی در ارتباطات و سیستم‌های اطلاعاتی برای افزایش درجه عدم قطعیت ممکن است به کار گرفته شود. پس از مدتی کارکنان نظامی اعتماد خود به سیستم‌های اطلاعاتی ازدست‌داده و به سمت سیستم‌های اطلاعاتی ناکارامدتری سویچ می‌کنند در این حالت شرایط عملیات اطلاعاتی جهت فریب فراهم می‌شود و اثربخشی ماموریت را تحت تاثیر قرار می‌دهد[۲٤] [٤۰] [۳۸] [۳٦].

**۲-۷-۵-۱. افزایش فریب اطلاعاتی ناشی از استفاده فنّاوری تجاری**

چنانچه در قسمت فنّاوری ذکرشده است بودجه‌های نظامی در حال کاهش است و بخش تجاری مسئول بیشتر پیشرفت‌های فنی است. در نتیجه یک نیروی شبکه‌ای شده مجبور است خود را با فنّاوری غیرنظامی تطبیق دهد. با توجه به ساختار امنیتی ضعیف‌تر و وجود رخنه‌های امنیتی، نهایتاً سیستم‌های نظامی آسیب‌هایی مشابه سیستم‌های غیرنظامی خواهند داشت [۲۷] [۲۸].

**۳-۷-۵-۱. ارتباط بین حسگرها به تیراندازان قابلیت فریب را افزایش می‌دهد.**

جنگ شبکه محور از ایده اتصال حس‌گر به تیراندازان پشتیبانی می‌کند که این مسئله استراتژی فریب را راحتر می‌کند؛ زیرا عملیات شبکه محور تمایل به کاهش زمان تصمیم‌گیری و کاهش تلاش برای تشخیص اهداف درست از نادرست است. پس آسیب‌پذیری در برابر فریب را افزایش می‌دهد که خود یکی از آسیب‌های جدی است [۲۷].

**۸-۵-۱. آسیب‌پذیری از ریسک و خطر بالقوه اطلاعاتی**

**۱-۸-۵-۱. شبکه می‌تواند باعث کاهش اطلاعات اشتراکی توسط افراد شود درنتیجه باعث از دست رفتن محتوی خواهد شد.**

در روش‌های مرسوم اطلاعات غالباً به‌صورت شخص-به-شخص انتقال می‌یابد که باعث انتقال کامل مفهوم و تفسیر درست از اطلاعات می‌شود؛ اما در محیط شبکه محوری ممکن است تفسیر غلطی از اطلاعات صورت پذیرد. هر چند با استفاده از متادیتا تا حدودی می‌توان مشکل را حل کرد اما این تنها درمان علائم است نه درمان کامل این مشکل [٤۱].

**۲-۸-۵-۱. شبکه می‌تواند باعث افزایش آشفتگی در محیط‌های ائتلافی شود.**

در حال حاضر جریان اطلاعات در محدوده هم‌پیمانان و دوستان به صورت محدود انجام می‌شود مثلاً از طریق دروازه‌های محدود یا افسران رابط. هرچند این مسئله موجب کاهش سرعت و تأخیر می‌شود اما تضمین می‌کند که تنها اطلاعات قابل تفسیر منتقل می‌شوند؛ اما

در یک محیط شبکه‌ای به دلیل بالا بودن حجم اطلاعات انتقالی، احتمال تفسیر نادرست و حتی ایجاد خصومت با دوستان بیشتر می‌شود [٤١].

**۹-۵-۱. آسیب‌پذیری‌های بالقوه از منظر فرماندهی**

**۱-۹-۵-۱. شبکه‌ها می‌توانند تأثیر نامطلوبی در تغییر تعادل بین فرماندهی و کنترل ایجاد کنند.**

دسترسی بیش از حد اطلاعات موجب تغییرات ناخواسته و نامطلوب در صلاحیت و اقتدار یک فرمانده می‌شود. به طور مثال به دست آوردن اطلاعات از نیروهای تحت امر موجب کنترل بیش از حد و مدیریت خُرد (جز به جز) توسط فرمانده می‌شود. برعکس در صورت تکیه بر اطلاعات عملیاتی و استراتژیک ممکن است واکنش‌های نامناسبی از طرف نیروهای تحت امر صورت پذیرد. پایه و اساس خودهمزمانی آن است که نیروهای تحت فرماندهی در چارچوب کلی اهداف مأموریت، خود اقدام به تصمیم‌گیری نمایند [۳۲] [٢٤] [٣٤].

**۲-۹-۵-۱. دسترسی به اطلاعات بسیار زیاد منجر به موقعیت تصمیم‌های نامناسب خواهد شد.**

با دسترسی بیشتر اطلاعات برای فرماندهان، این مزیت وجود خواهد داشت که در محل‌هایی که قبلاً امکان تصمیم‌گیری وجود نداشت اکنون فراهم شده است؛ اما آسیب‌پذیری این مسئله در جایی است که افرادی غیرمسئول، غیر کاردان، ناآگاه و آموزش ندیده ممکن است تصور کنند به دلیل داشتن اطلاعات، قادر به تصمیم‌گیری. هستند [۳۲] [٣٤]

**۳-۹-۵-۱. برتری تصمیم‌گیری و سرعت منجر به اضافه‌کاری و خستگی نیروها خواهد شد.**

نیاز به جمع‌آوری اطلاعات و برتری در تصمیم‌گیری به همراه سرعت بالا، ممکن است حجم و بارکاری را بالا ببرد. اگر این سیکل تصمیم‌گیری و ارزیابی پرسرعت ادامه‌دار باشد ممکن است منجر به فرسوده شدن تیم فرماندهی گردد. جنگ شبکه محور ممکن است برای افزایش هماهنگی، حجم یا بارکاری را افزایش دهد درنتیجه باعث افزایش استرس خواهد شد. این استرس ممکن است به سطحی بحرانی رسیده و موجب کاهش سریع تأثیر فرمانده شود [٢٤] [۳۲] [٣٤].

**٤-۹-۵-۱. دسترسی اطلاعات بیشتر منجر به تصمیمات ضعیف خواهد شد.**

فرضیهٔ «داشتن اطلاعات بیشتر تصمیم‌گیری را بهینه می‌نماید» اثبات نشده است. افزایش اطلاعات ممکن است گاهی منجر به طرح نقشه غیرمنعطف و شکننده شود. دلیل آن این است که در شرایطی که عدم قطعیت بالاست فرمانده سعی می‌کند تصمیمات انعطاف‌پذیرتری بگیرد اما زمانی که اطلاعات زیادی وجود نداشته باشد تصمیمات فرمانده نیز قطعی‌تر و با جزئیات بیشتر است [۳۲].

**۵-۹-۵-۱. اعتماد به برتری اطلاعاتی**

مفهوم کلی عملیات بر پایه آن است که شبکه، کلیه اطلاعات مورد نیازمان را در اختیار قرار می‌دهد. حال آنکه ممکن است گاهی این‌گونه نباشد و در موقعیتی باشیم که دچار فقر اطلاعاتی شویم مثلاً درگیر یک جنگ خیابانی در کشوری باشیم که با زبانش آشنا نیستیم، فرهنگشان را نمی‌شناسیم و بخش زیادی از افراد محلی به ما اعتماد ندارند [٤٢].

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ۱، بهار ۱۳۹۷

**۱۰-۵-۱. آسیب‌پذیری از منظر جنگ الکترونیک**

در قرن بیستم، جنگ الکترونیکِ حوزه راداری بسیار برجسته و پررنگ بوده است به‌طوری‌که نقش آگاهی وضعیتی و محافظت از سکوهای نظامی به‌عنوان نقش اصلی جنگ الکترونیک تعریف شده بود؛ اما در قرن بیست یکم ناتو برای جنگ الکترونیک مخابراتی نقش آگاهی طیفی و محافظت از شبکه را برای جنگ شبکه محور برجسته نموده است [۴۳]. از نگاه ناتو با توجه به رویکرد محافظتی، آسیب‌پذیری‌های جنگ الکترونیک، چالش‌های بسیار زیادی را برای جنگ شبکه محور دارد.

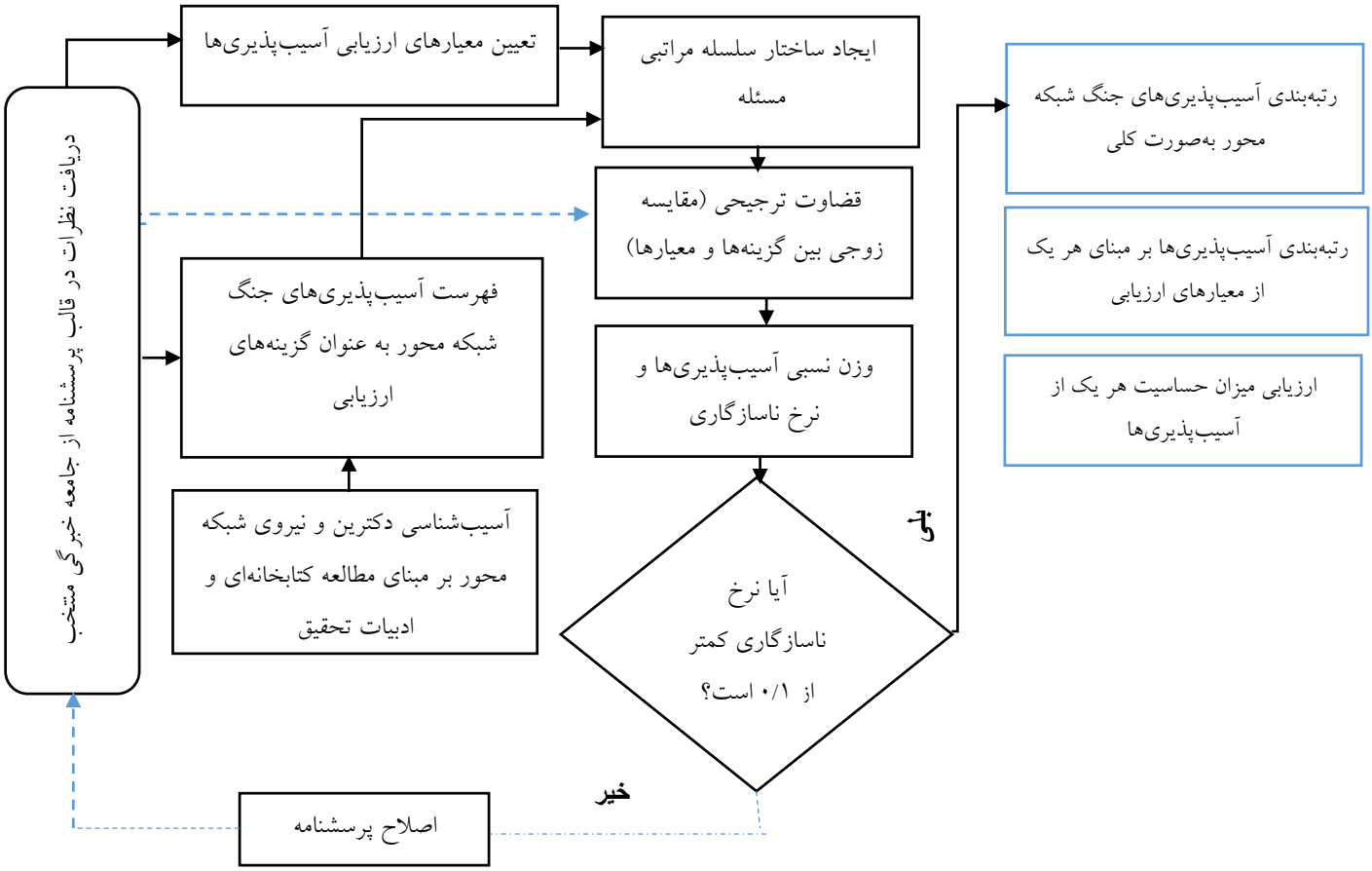
**۶-۱. روش‌شناسی تحقیق**

این تحقیق از نظر هدف کاربردی است. شیوه تحقیق بر اساس تجزیه وتحلیل اسناد (مطالعه کتابخانه‌ای) مربوط به مطالعات موردی عملیات شبکه محور آمریکا در رزمایش‌ها و آسیب‌پذیری‌های عملیات شبکه محور از منابع آشکار بوده است. در این پژوهش با توجه به شکل (۲) الگویی بر مبنای فرایند تحلیل سلسه مراتبی، به ارزیابی و رتبه‌بندی آسیب‌های عملیات شبکه محور پرداخته شده است. سپس با ایجاد یک پنل خبرگان کاملاً هدفمند و انتخاب شده از فرماندهان ارشد نظامی در سطح عملیات، اطلاعات و پشتیبانی که دارای مدارک دانشگاهی در سطح دکتری، دانشجوی دکتری و کارشناسی ارشد بوده دو فعالیت زیر انجام شده است:

الف) تعیین و تأیید دسته‌بندی آسیب‌پذیری‌های جنگ شبکه محور؛ با توجه به آنکه آسیب‌های جزئی، در این صحنه نبرد پیچیده می‌تواند تأثیرات شگرفی داشته باشند، عملاً حذفی از آسیب‌پذیری‌ها انجام نشده است و در مواردی آسیب‌ها در هم ادغام و یا در دسته‌های دیگر جابجا شدند. به‌طور مثال آسیب‌پذیری‌های اجتماعی با توجه ویژگی‌هایشان در حوزه آسیب‌های نیروی انسانی ادغام شده است. همچنین آسیب‌پذیری از منظر جنگ الکترونیک/سایبرالکترونیک در این پژوهش نیز بسیار برجسته شده است. تصمیم‌گیری برای تعیین و تأیید دسته‌بندی بر مبنای قضاوت خبرگان و رائ اکثریت بوده است.

ب) تعیین معیارهای ارزیابی آسیب‌پذیری در محیط پیچیده و پویا جهت استفاده مناسب نیروهای مسلح ج.ا.ا. در این پنل معیارها از نگاه کاربردی و عملیاتی در جهت استفاده مؤثر انتخاب شده است. برای این منظور ابتدا معیارهای ارزیابی از منظرهای مختلف از خبرگان منتخب جمع‌آوری شد و سپس با پرسش آنکه این معیارها می‌تواند معیار مؤثری باشد تصمیم‌گیری اکثریت شده است. احتمال انتخاب معیارهای ارزیابی در این تحقیق در گام نهایی تقریباً یک (بیش از ۹۵٪) بوده که اثبات روایی و صحت آن می‌باشد. برای اعتبار معیارهای ارزیابی بر مبنای پرسشنامه طیف لیکرت از یک جامعه منتخب ۳۲ نفره استفاده شده است. ضریب آلفای کرونباخ ۰/۸۲ معیار پایایی معیارهای ارزیابی می‌باشد.

ج) اعتبار و پایایی نظرات خبرگان منتخب جهت تکمیل پرسشنامهٔ مقایسات زوجی میزان نرخ ناسازگاری کمتر از ۰/۱ است؛ که در تمامی مراحل ارزیابی و پیاده‌سازی، این سطح آستانه رعایت شده است (نرخ سازگاری در این پژوهش به طور متوسط ۰/۰۸ است). برای رسیدن به این معیار چندین بار مقادیر توسط خبرگان منتخب (۷ نفر منتخب) اصلاح شده است. برای سهولت




شکل ۲: مدل ارزیابی پیشنهادی بر مبنای تحلیل سلسله مراتبی



پیاده‌سازی پژوهش از نرم‌افزار Expert Choices استفاده شده است و از میانگین هندسی نظرات خبرگان منتخب استفاده شده است.

زمان انجام این پژوهش و استفاده از نظر خبرگان نظامی که غالب آن‌ها در حوزه سایبر الکترونیک می‌باشند زمستان ۱۳۹۶ است.

### ۷-۱. سازماندهی تحقیق

ساختار این تحقیق در چهار بخش تنظیم شده است. بخش اول شامل بیان مسئله، ضرورت و اهمیت، پرسش، هدف، پیشینه و روش تحقیق است. در بخش دوم به مبانی نظری شامل مفاهیم مرتبط با جنگ شبکه محور، آسیب‌شناسی و فرایند تحلیل سلسله مراتبی اشاره شده است. بخش سوم شامل مدل‌سازی مسئله و شبیه‌سازی فرایند تحلیل آسیب‌پذیری‌ها، یافته‌های تحلیل است. بخش نهایی شامل نتیجه‌گیری و پیشنهادها برای کارهای آتی است.

## ۲. ادبیات و مبانی نظری تحقیق

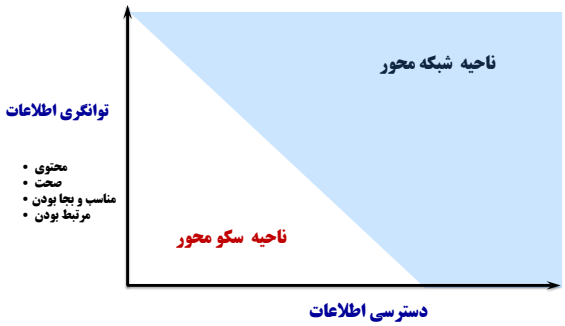
رویکرد شبکه محوری، تجسم نظامی از مفهوم جنگ در عصر اطلاعات است. مطالعات نشان داده که شبکه‌سازی

نیروها را قادر می‌سازد دامنه وسیع‌تری از مأموریت‌ها را نسبت به حالتی که شبکه نیستند متقبل شوند. این توانمندی توسط بهبود کارایی و اثربخشی ایجاد می‌شود. جنگ شبکه محور با استفاده از پیوند دادن بین کامپیوترها و ارتباطات مردم از طریق جریان اطلاعات شکل می‌گیرد. این ارتباط بستگی به قابلیت همکاری سامانه‌های استفاده شده توسط نیروی نظامی ارتش آمریکا است [۸].

### ۱-۲. تعریف عملیاتی از جنگ/ عملیات شبکه محور[۲۷]

۱- عملیات شبکه محور یعنی بهره‌برداری از مزایای شبکه انسان و فناوری؛ از کلیه عناصر یک نیروی مشرک تعلیم دیده و کاملاً یکپارچه در؛ توانمندی‌ها، آگاهی، دانش، تجربه و تصمیم‌گیری برتر، برای دست‌یابی به سطح بالایی از چابکی و اثربخشی در وضعیت‌های پراکنده، غیرمتمرکز، پویا و نامطمئن محیط‌های ائتلافی [۹]؛

۲- عملیات شبکه محور یک عملیات نظامی است که به‌وسیله شبکه‌ای شدن نیروها امکان‌پذیر است و مطابق شکل (۳) دستیابی به ناحیه جدیدی از دامنه اطلاعات که قبلاً دست‌نیافتنی بوده را ممکن می‌سازد. این نوع عملیات، جنگجویان را به نوع جدیدی از برتری اطلاعاتی مجهز می‌کند. این برتری عمدتاً با استفاده از قابلیت‌های به اشتراک‌گذاری و افزایش دستیابی به اطلاعات، مشخص می‌شود [۱].




**شکل ۳: دسترسی اطلاعات در ناحیه شبکه محوری [۱]**

در این پژوهش به‌مانند اکثر اسناد تعریف عملیاتی از عملیات شبکه محور و جنگ شبکه محور به‌جای هم استفاده خواهد شد[۲۸] و لذا تعریف عملیاتی آن نیز به‌صورت زیر است:

یک مفهوم برتری اطلاعاتی[۲۹] در عملیات است که با حسگرهای شبکه‌شده، تصمیم‌گیرندگان، اجراکنندگان (تیراندازان)، توان رزمی را افزایش داده و می‌تواند به آگاهی مشترک، سرعت فرماندهی، سرعت بالاتر عملیات، کشندگی و مرگ‌آوری بیشتر و افزایش مقاومت در مقابل دشمن و درجه‌ای از خود هم‌زمانی[۳۰] دست یابد [۱۰].

### ۱-۱-۲. اصول و انگاره‌های جنگ شبکه محور

چهار اصل و انگاره اساسی از جنگ شبکه محور و مجموعه‌ای از اصول حاکم از نیروی شبکه محور مشخص‌شده است. این اصول به عنوان هسته جنگ شبکه محور و تئوری نوظهور از جنگ در عصر اطلاعات است. این اصول در فهم، افزایش قدرت یک نیروی شبکه‌ای شده کمک می‌کند. همچنین این اصول فرضیه

[۲۷] Network Centric Operation

[۲۸] برای نمونه مهم‌ترین سند از این نظر، گزارش به کنگره آمریکا در مورد جنگ شبکه محور است

[۲۹] Information superiority

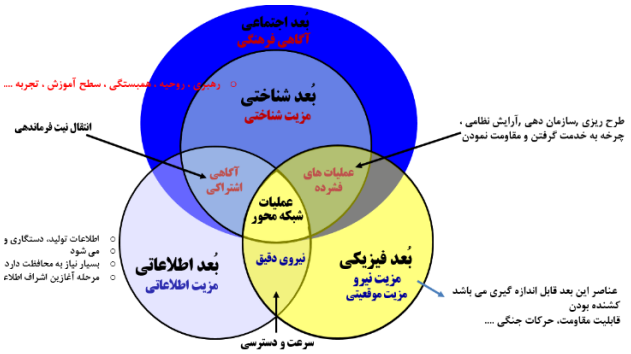
[۳۰] Self-Synchronization

جنگ شبکه محور به‌عنوان منبع «مزیت جنگی[۳۱]» را شکل می‌دهد که عبارت‌اند از:

۱. یک نیروی شبکه شده قوی اشتراک اطلاعات را بهبود می‌بخشد.
۲. اشتراک اطلاعات و تعاملات باعث افزایش کیفیت اطلاعات و آگاهی وضعیتی مشترک می‌شود.
۳. آگاهی وضعیتی مشترک باعث فراهم نمودن تعاملات و خودهمزمانی می‌شود. درنتیجه افزایش مقاومت در مقابل دشمن و سرعت در فرماندهی را به همراه دارد.
٤. پس به‌صورت چشمگیری اثربخشی مأموریت افزایش خواهد یافت.

### ۲-۱-۲. بُعدهای[۳۲] جنگ شبکه محور

جنگ شبکه محور شامل شبکه‌سازی در چهار بُعد؛ شامل بُعد فیزیکی، اطلاعاتی، شناختی و اجتماعی، است [۱۱]. بُعد اجتماعی توسط موسسه تحقیقاتی رند[۳۳] توسعه‌یافته است. شرح وظایف هر یک از بُعدها در جنگ شبکه محور در شکل (٤) نشان داده شده است.




**شکل ٤: مدل مفهومی جنگ شبکه محور بر مبنای بُعدهای آن [۱۱]**

### ۳-۱-۲. توانمندی و قابلیت‌های جنگ شبکه محور

با توجه به بررسی مفهوم شبکه محوری و جنگ شبکه محور در منابع آشکار، می‌توان توانمندی و قابلیت‌های زیر برای یک نیروی شبکه محور در نظر گرفت:

۱. افزایش توانمندی با ارتباط مؤثر بین منابع و موجودی‌های یک نیرو در میدان نبرد؛
۲. قابلیت بهره‌گیری از یک نیروی نظامی که ازنظر جغرافیایی دارای پراکندگی وسیعی باشد؛
۳. برخورداری از یک نیروی نظامی آگاه و هوشمند؛
٤. ایجاد اشراف و برتری اطلاعاتی در صحنه نبرد؛
۵. افزایش آگاهی موقعیت از صحنه نبرد؛
٦. چابکی و سرعت در فرماندهی؛
۷. امکان اجرای عملیات ضربتی و برق‌آسا؛
۸. تخصیص بهتر منابع؛
۹. امکان هجوم دسته‌جمعی[۳٤]؛
۱۰. فرماندهی غیرمتمرکز و توزیع‌شده (استفاده در جنگ‌های نامتقارن)؛
۱۱. آشکارسازی سریع‌تر تهدیدات؛
۱۲. کاهش هزینه و ریسک؛

## ۲-۲. الگوی پیشنهادی برای حل مسئله تحقیق

در این تحقیق مسئله و سؤال اساسی روشی برای ارزیابی آسیب‌های جنگ/عملیات شبکه محور است. با توجه به تعداد آسیب‌ها و همچنین تعداد معیارهایی که در ارزیابی آسیب‌ها نقش ایفا می‌کنند آن را به یک مسئله پیچیده تبدیل نموده است. همچنین می‌دانیم در علم تصمیم‌گیری، انتخاب یک راهکار یا گزینه از بین راهکارهای موجود یا اولویت‌بندی راهکارها مطرح است و چند سالی است که روش‌های تصمیم‌گیری با

[۳۱] Warfighting Advantage
[۳۲] Domain
[۳۳] RAND
[۳٤] Swarming

معیارهای چندگانه[35] جای خود را باز کرده است. از این میان روش تحلیل سلسله مراتبی بیش از سایر روش‌ها در علم مدیریت مورد استفاده قرارگرفته است. فرایند تحلیل سلسله مراتبی[36] یکی از معروف‌ترین فنون تصمیم‌گیری چند شاخصه است که اولین بار توسط توماس آل ساعتی عراقی الاصل در دهه ۱۹۷۰ ابداع گردید [۴۳]. فرایند تحلیل سلسله مراتبی منعکس کننده رفتار طبیعی و تفکر انسانی است. این تکنیک، مسائل پیچیده را بر اساس آثار متقابل آن‌ها مورد بررسی قرار می‌دهد و آن‌ها را به شکلی ساده تبدیل کرده و به حل آن می‌پردازد.

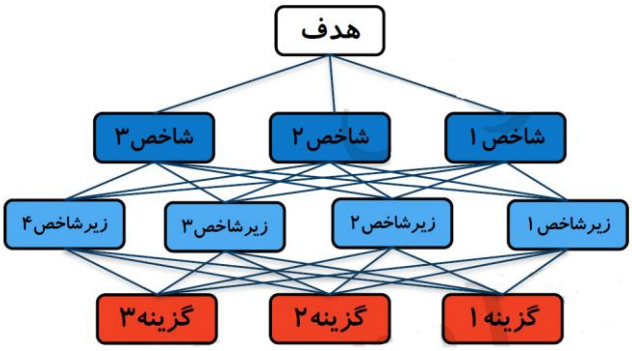
در این مرحله، مدل‌سازی مسئله به‌صورت سلسله مراتبی از عناصر تصمیم که با هم در ارتباط می‌باشند، ایجاد می‌شود. عناصر تصمیم شامل «معیارهای تصمیم‌گیری» و «گزینه‌های تصمیم» است. با توجه به روش تحلیل فرایند سلسه مراتبی الگوی حل مسئله پژوهش در پنج مرحله کلی انجام می‌شود؛ که شامل ورودی‌های لازم مدل، مدل‌سازی مساله پژوهش بر اساس ساختار فرایند تحلیل سلسله مراتبی، مقایسه‌های زوجی، محاسبه وزن نسبی آسیب‌پذیری و رتبه‌بندی آسیب‌پذیری‌ها است که هر یک از مراحل را به اختصار توضیح داده می‌شود.

### ۲-۲-۱. ورودی‌های لازم مدل

این مرحله شامل تعیین هدف، شاخص‌های اندازه‌گیری و گزینه مسئله پژوهش است. هدف مسئله پژوهش ارزیابی و رتبه‌بندی آسیب‌پذیری‌های عملیات شبکه محور است. شاخص‌های ارزیابی آسیب‌های عملیات شبکه محور توسط خبرگان استخراج و مورد تأیید قرار می‌گیرد. گزینه‌های مسئله که آسیب‌پذیری‌های عملیات شبکه محور است توسط جمع‌آوری اسناد و مطالعات کتابخانه‌ای استخراج و دسته‌بندی این آسیب‌ها مورد تأیید خبرگان منتخب قرار گرفته است.

### ۲-۲-۲. مدل‌سازی مسئله پژوهش بر اساس ساختار سلسه مراتبی

فرایند تحلیل سلسله مراتبی مطابق شکل (۵)، نیازمند شکستن یک مسئله به چندین معیار یا شاخص به سلسله مراتبی از سطوح است. سطح بالا بیانگر هدف اصلی فرایند تصمیم‌گیری است. سطح دوم، نشان دهنده معیار یا شاخص‌ها عمده و اساسی که ممکن است به زیرمعیارهای فرعی و جزئی‌تر در سطح بعدی شکسته، است. سطح آخر گزینه‌های تصمیم را ارائه می‌کند؛




شکل ۵: ساختار سلسله مراتب تصمیم

### ۲-۲-۳. قضاوت ترجیحی (مقایسه‌های زوجی)

انجام مقایسه بین گزینه‌های مختلف تصمیم، بر اساس هر معیار و قضاوت در مورد اهمیت معیارهای تصمیم با انجام مقایسه‌های زوجی، بعد از طراحی سلسله‌مراتب مسئله تصمیم انجام می‌شود. تصمیم گیرنده می‌بایست مجموعه ماتریس‌هایی که به‌طور عددی اهمیت یا

[35] Multi– Criteria Decision Making (MCDM)

[36] Analytic Hierarchy Process (AHP)

ارجحیت نسبی معیارها را نسبت به یکدیگر و هر گزینه تصمیم را با توجه به معیارها نسبت به سایر گزینه‌ها اندازه‌گیری می‌نماید، ایجاد کند. برای انجام این کار معمولاً از مقایسه گزینه‌ها با معیارهای i ام نسبت به گزینه‌ها یا معیارهای j ام استفاده می‌شود که در جدول زیر نحوه ارزش‌گذاری معیارها نسبت به هم نشان داده شده است.

جدول ۲: جدول قضاوت توماس آل ساتی [۴۳]

| وزن | تعریف | توضیح |
|---|---|---|
| ۱ | برابر اهمیت | یکسان (شاخص) بااهمیت دو فعالیت |
| ۳ | معمولی اهمیت (نسبتاً مهم‌تر) | فعالیت بر فعالیت یک نفع به نظر و تجربه برتر) دیگر (کمی |
| ۵ | بسیار اهمیت (مهم‌تر) | بر فعالیت یک برتری مورد در نظر و تجربه زیاد) دیگر (برتری فعالیت |
| ۷ | بسیار زیاد اهمیت (خیلی مهم‌تر) | فعالیت دیگر بر بیشتری بسیار اهمیت فعالیت، یک اثبات‌شده است عمل در آن اهمیت و دارد |
| ۹ | فوق‌العاده اهمیت (کاملاً مهم) | بر فعالیت را فعالیت یک فوق‌العاده اهمیت شواهد، اهمیت که این می‌شود تأیید و می‌دهد نشان دیگر دارد وجود |
| ۲،٤،٦، ۸ | بین مقایسه برای مقادیر بالا | انجام شود، تلفیقی عددی، مقایس‌های داوری یک وجود ندارد توصیف برای خوبی کلمه زیرا |

### ۲-۲-٤. محاسبات وزن‌های نسبی

قدم بعدی در فرایند تحلیل سلسله مراتبی انجام محاسبات لازم برای تعیین اولویت هر یک از عناصر تصمیم و یا وزن شاخص‌ها با استفاده از اطلاعات ماتریس‌های مقایسه‌های زوجی است. از میان روش‌های محاسبه مقادیر وزنی روش‌هایی چون میانگین حسابی، میانگین هندسی بیشترین استفاده را از میان روش‌های دیگری چون حداقل مربعات، روش مجموع سطری و روش مجموع ستونی می‌باشند.

### ۲-۲-۵. ادغام وزنهای نسبی

به‌منظور رتبه‌بندی گزینه‌های تصمیم، در این مرحله بایستی وزن نسبی هر عنصر را در وزن عناصر بالاتر ضرب کرد تا وزن نهایی آن به دست آید. با انجام این مرحله برای هر گزینه، مقدار وزن نهایی به دست می‌آید.
سپس مقدار وزن گزینه‌ها در تمام شاخص‌ها با یکدیگر جمع خواهد شد تا ارزش نهایی گزینه استخراج شود.

### ۲-۲-٦. سازگاری در قضاوت‌ها

تقریباً تمامی محاسبه‌های مربوط به فرایند تحلیل سلسله مراتبی بر اساس قضاوت اولیه تصمیم‌گیرنده که در قالب ماتریس مقایسه‌های زوجی ظاهر می‌شود، صورت می‌پذیرد. هرگونه خطا و ناسازگاری در مقایسه و تعیین اهمیت بین گزینه‌ها و معیارها نتیجه نهایی به‌دست‌آمده از محاسبات را مخدوش می‌سازد. نرخ ناسازگاری[۳۷] وسیله‌ای است که سازگاری را مشخص ساخته و نشان می‌دهد که تا چه حد می‌توان به اولویت‌های حاصل از مقایسه‌ها اعتماد کرد. شاید مقایسه دو گزینه امری ساده باشد، اما وقتی‌که تعداد مقایسه‌ها افزایش یابد اطمینان از سازگاری مقایسه‌ها به‌راحتی میسر نبوده و باید با به‌کارگیری نرخ سازگاری به این اعتماد دست‌یافت. تجربه نشان داده است که اگر نرخ ناسازگاری کمتر از ۰/۱۰ باشد سازگاری مقایسه‌ها قابل قبول بوده و در غیر این صورت مقایسه‌ها باید تجدید نظر شود.

## ۳. پیاده‌سازی مدل، تجزیه تحلیل داده‌ها و یافته‌های تحقیق

مراحل اجرایی پژوهش و مدل‌سازی به صورت گام‌های زیر است:

[۳۷] Inconsistency Ratio (I.R)

**مرحله اول: استخراج آسیب‌پذیری‌های جنگ شبکه محور آمریکا**

با توجه به ادبیات پژوهش و پیشینه تحقیق آسیب‌پذیری‌ها بررسی‌شده و دسته‌بندی اولیه شده است. دسته‌بندی این آسیب‌پذیری‌ها در این پژوهش با تأیید خبرگان در یک جلسه اندیشه‌ورزی، مطابق جدول (۳) مورد بررسی و تأیید قرارگرفته است. با توجه نظر خبرگان منتخب، ویژگی‌های آسیب‌پذیری تعامل اجتماعی در درون معیار نیروی انسانی در نظر گرفته‌شده است. تأیید آسیب‌پذیری با توجه به آنکه آسیب‌های جزئی در این صحنه پیچیده می‌توان اثر شگرفی داشته باشد با کمترین حذف صورت پذیرفته و فقط در چند مورد مصادیق آسیب‌پذیری جابجا شده است. مبنای تأیید نظر اکثریت خبرگان منتخب بوده است و میزان تأیید هر یک از آن‌ها بیش از ۹۰٪ بوده است.

جدول ۳: آسیب‌پذیری‌های جنگ شبکه محور

| | آسیب‌پذیری‌ها | مصادیق آسیب‌پذیری |
|---|---|---|
| ۱ | پیشرفت علوم | ○ علوم پیچیدگی؛ مدل‌سازی صحنه نبرد بر مبنای رفتار انطباقی سیستم پیچیده<br>○ اثرات شبکه‌ای مانند استخراج نودهای مؤثر<br>○ مدل‌سازی صحنه نبرد بر مبنای تئوری سیستم‌ها<br>○ استخراج نقاط ضعف بر مبنای نظریه‌های فلسفی (تفکیک مفاهیم و تحلیل مجرد هر یک از آن‌ها...) |
| ۲ | فنّاوری | ○ عدم تقارن فنّاوری در نیروهای ائتلاف غربی<br>○ محدودیت‌های فنّاوری مانند پهنای باند<br>○ استفاده از فنّاوری‌های تجاری<br>○ رسوب دانش در حوزه فن‌آوری |
| ۳ | شبکه و ارتباطات | ○ نبود شبکه مرجع و جامع و ضعف در پشتیبانی از آن‌ها<br>○ سطوح امنیتی مختلف در میان شبکه‌ها |
| ٤ | نیروی انسانی | ○ کم‌رنگ شدن نقش نظارتی نیروی انسانی<br>○ کاهش تعامل اجتماعی<br>○ فرسایشی شدن جنگ و کاهش اثربخشی نیرو |
| ٥ | فرماندهی | ○ دسترسی بیش‌ازحد اطلاعات و تأثیرات نامطلوب آن<br>○ برتری تصمیم‌گیری و سرعت موجب خستگی و فرسایش تیم فرماندهی می‌شود<br>○ دسترسی به اطلاعات فراوان احتمال تصمیمات ضعیف را کاهش نمی‌دهد<br>○ اعتماد بیش از حد به برتری اطلاعاتی |
| ٦ | محیط اطلاعاتی جدید | ○ افزایش سرعت و کاهش زمان‌پاسخدهی<br>○ افزایش بار اطلاعاتی، سرعت، افزایش کشندگی یک ترکیب خطرناک<br>○ افزایش عدم قطعیت و کاهش زمان‌پاسخدهی |
| ۷ | پردازش اطلاعات | ○ تصویر عملیاتی مشترک و فقدان نمایش واقعیت از صحنه نبرد<br>○ مدیریت اطلاعات و افزایش عدم قطعیت<br>○ اتکای بیش از حد به زیرساخت‌های اطلاعاتی و نبود توانایی جهت حالت‌های جایگزین |
| ۸ | ریسک و خطرات اطلاعات | ○ کاهش اطلاعات مشترک و از دست رفتن محتوی<br>○ کاهش آگاهی و عدم هماهنگی<br>○ افزایش آشفتگی در محیط‌های ائتلافی |
| ۹ | فریب اطلاعات | ○ افزایش خطرپذیری با عملیات اطلاعاتی (اشکلات تصادفی، ... و کاهش اعتماد).<br>○ افزایش فریب اطلاعاتی ناشی از استفاده از فنّاوری‌های تجاری<br>○ ارتباط بین حسگرها به تیراندازن و افزایش قابلیت فریب |
| ۱۰ | جنگ/ سایبرالکترونیک | ○ آسیب‌پذیری قابلیت‌های جنگ الکترونیک و اثرمستقیم در کاهش اثربخشی مأموریت |

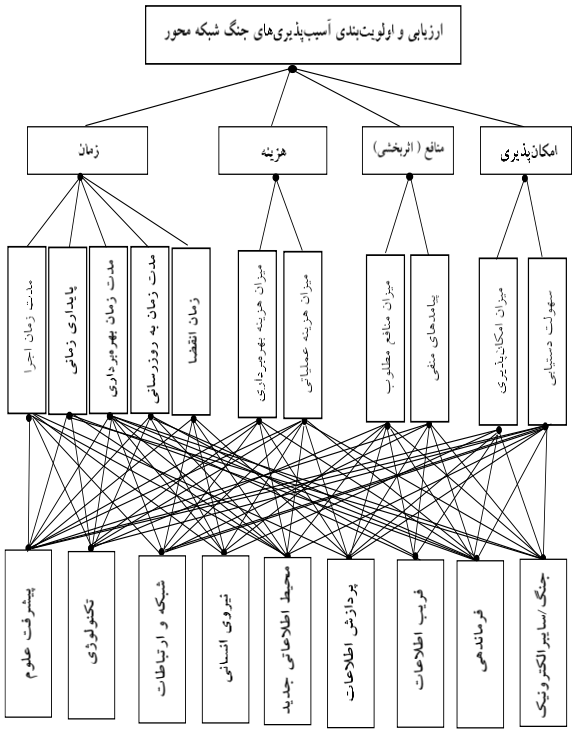
**مرحله دوم: استخراج شاخص‌های ارزیابی آسیب‌شناسی جنگ شبکه محور بر مبنای نظرات خبرگان**

با تشکیل پنلی از خبرگان از فرماندهان ارشد در سِمت‌های عملیاتی، اطلاعاتی، لجستیک، معیارهای جدول (٤) به عنوان معیارهای کاربردی برای ارزیابی آسیب‌پذیری جهت استفاده مؤثر نیروهای مسلح ایران، استخراج شده است. تعدادی از زیرمعیارها توسط خبرگان با توجه به اهمیت کم آن‌ها تأیید نشده‌اند؛ مانند زیرمعیارهایی چون امکان‌پذیری بروزرسانی و میزان هزینه لازم برای بروزرسانی حذف شده است. سپس پایایی و اعتبار این شاخص‌ها توسط ۳۲ خبره منتخب بر مبنای ضریب آلفای کرونباخ ۰/۸۲ مورد ارزیابی و تأیید قرار گرفت.

جدول ٤: معیارها و زیرمعیارهای ارزیابی آسیب‌پذیری جنگ شبکه محور

| | معیار | زیرمعیارها |
|---|---|---|
| ۱ | زمان | ۱- **مدت زمان اجرا** (زمان لازم برای رسیدن به آسیب‌پذیری)<br>۲- **پایداری زمانی** (پایداری زمانی جهت استفاده از آسیب‌پذیری)<br>۳- **مدت زمان بهره‌برداری** (مدت زمان لازم برای رسیدن به مرحله بهره‌برداری از آسیب‌پذیری)<br>٤- **مدت زمان بروزرسانی** (مدت زمان بروزرسانی برای ظروف مختلف جهت استفاده از آسیب‌پذیری)<br>۵- **زمان انقضا** (مدت زمان استفاده از آسیب‌پذیری) |
| ۲ | هزینه | ۱- میزان **هزینه لازم برای رسیدن** و کشف آسیب‌پذیری<br>۲- **میزان هزینه برای عملیاتی‌شدن** از آسیب‌پذیری |
| ۳ | اثر بخشی | ۱- **میزان منافع** حاصل از استفاده از آسیب‌پذیری<br>۲- **پیامدهای منفی** حاصل از به‌کارگیری آسیب‌پذیری |
| ٤ | امکان‌پذیری | ۱- **میزان امکان‌پذیری** (به‌کارگیری) آسیب‌پذیری<br>۲- **تسهیل دستیابی** به بهره‌برداری از آسیب‌پذیری |

**مرحله سوم: ساخت سلسله‌مراتب اولویت‌بندی آسیب‌های جنگ شبکه محور برمبنای تحلیل سلسله**




شکل ٦: ساخت سلسله مراتب تصمیم پژوهش

**مراتبی**

با توجه به مدل‌سازی مسئله که از سه بخش هدف، معیار یا شاخص و گزینه تشکل شده، ساختار سلسله مراتبی مسئله پژوهش به صورت شکل (٦) مدل می‌شود.

**مرحله چهارم: قضاوت ترجیحی (مقایسه‌های زوجی بین گزینه‌ها و معیارها توسط نرم‌افزار)**

برای مقایسه‌های زوجی با توجه به تعداد زیاد حالت‌های استفاده نمودیم. با Expert Choicesمقایسه‌ها از نرم‌افزار استفاده از نظر کارشناسان خبره نظامی و به صورت هدفمند (۷ نفر) حدوداً با حداقل ۲۵ سال تجربه و مدرک تحصیلات تکمیلی کارشناسی ارشد و دکتری با تکمیل پرسشنامه مقایسه‌های زوجی انجام شده است.

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ۱، بهار ۱۳۹۷

**مرحله پنجم: محاسبه‌های وزن‌های نسبی گزینه‌ها و بررسی نرخ ناسازگاری کمتر از ۰/۱۰**

با استفاده از نرم‌افزار محاسبات وزنی گزینه‌ها محاسبه می‌شود. در هر مرحله میزان ضریب ناسازگاری بررسی می‌شود که مبنای درستنمایی داده‌های ورودی است. در این پژوهش نرخ ناسازگاری به طور میانگین ۰/۰۷ می‌باشد. در موارد بسیار زیادی که نرخ ناسازگاری بیش از ۰/۱ شده بود، پرسشنامه و یا به عبارتی مقایسه‌های زوجی بازبینی و تغییر یافته است.

**مرحله ششم: رتبه‌بندی آسیب‌پذیری‌های جنگ شبکه محوری**

آسیب‌پذیری‌های جنگ شبکه محور از منظرهای مختلف مورد ارزیابی و رتبه‌بندی قرار گرفته است؛ که تحلیل دقیق آن در بخش بعدی ارائه شده است.

## ٤. تحلیل داده‌ها و یافته‌های پژوهش

### ٤-١. رتبه‌بندی کلی آسیب‌پذیری جنگ شبکه محور

طبق تحلیل داده از منظر خبرگان، میزان وزنی هر یک از معیارهای ارزیابی مطابق جدول ۵ است.

جدول ۵: مقادیر وزنی معیارها و زیرمعیارها

| معیارها | زمان | | | | | هزینه | | اثربخشی | | امکان‌پذیری | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| وزن | ٪۱۳/٦ | | | | | ٪۲۸/۷ | | ٪۳۲/۷ | | ٪۳٤ | |
| زیرمعیارها | مدت‌زمان بروزرسانی | مدت‌زمان بهره‌برداری | زمان انقضا | پایداری زمانی | مدت‌زمان اجرا | هزینه عملیاتی شدن | هزینه بهره‌برداری | میزان منافع مطلوب | پیامدهای منفی | سهولت دستیابی | میزان امکان‌پذیری |
| مقادیر وزنی | ٪۱٤/٤ | ٪۱۵/۸ | ٪۳۲/۲ | ٪۲۹/۵ | ٪۸ | ٪۵۰ | ٪۵۰ | ٪۵۰ | ٪۵۰ | ٪۲۵ | ٪۷۵ |

بر اساس آسیب‌پذیری‌ها و طبق معیارهای ارزیابی تعریف شده، آسیب‌پذیری‌هایی از منظر جنگ الکترونیک، فنّاوری، آسیب‌پذیری‌های فرماندهی از آسیب‌های جدی شبکه محور است. نرخ ناسازگاری ۰/۰۷ است که نشان‌دهنده صحت ارزیابی و مقایسه‌ها است.

جدول ٦: مقادیر وزنی آسیب‌پذیری‌ها

| نرخ ناسازگاری: ۰/۰۷ | | |
|---|---|---|
| رتبه | مقادیر وزنی | آسیب‌پذیری |
| ۲ | ۰/۱۲۳ | فنّاوری |
| ۵ | ۰/۱۰۳ | علوم (پیچیدگی ...) |
| ٦ | ۰/۱۰۳ | شبکه و ارتباطات |
| ۷ | ۰/۰۹٤ | نیروی انسانی |
| ۱۰ | ۰/۰۵۸ | محیط جدید |
| ۹ | ۰/۰۷۱ | پردازش اطلاعات |
| ٤ | ۰/۱۱٤ | خطرات اطلاعات |
| ۸ | ۰/۰۸٦ | عملیات اطلاعاتی |
| ۱ | ۰/۱۲۸ | جنگ الکترونیک |
| ۳ | ۰/۱۲۱ | فرماندهی |

### ٤-٢. رتبه‌بندی آسیب‌پذیری از منظر زمان

از منظر زمان، آسیب‌پذیری‌هایی چون جنگ الکترونیک، فنّاوری و نیروی انسانی دارای بالاترین رتبه‌بندی از منظر زمان است. همچنین برای استفاده از آسیب‌پذیری‌هایی چون پیشرفت‌های علوم که مدل‌سازی رفتاری صحنه نبرد است نیاز به زمان بیشتری نسبت به سایر آسیب‌پذیری‌ها است.

جدول ۷: مقادیر وزنی آسیب‌پذیری‌ها از منظر زمان

| نرخ ناسازگاری: ۰/۰۹<br>میزان وزن در آسیب‌پذیری: ۰/۱۳٦ | | |
|---|---|---|
| رتبه | مقادیر وزنی | آسیب‌پذیری |
| ۲ | ۰/۱۵۱ | فنّاوری |
| ۹ | ۰/۰۵۳ | علوم (پیچیدگی ...) |
| ٤ | ۰/۱۰۹ | شبکه و ارتباطات |
| ۳ | ۰/۱۳۹ | نیروی انسانی |
| ۸ | ۰/۰۵۸ | محیط جدید |
| ۷ | ۰/۰۸۲ | پردازش اطلاعات |
| ۵ | ۰/۱۰۰ | خطرات اطلاعات |
| ٦ | ۰/۰۹۰ | عملیات اطلاعاتی |
| ۱ | ۰/۱۷۱ | جنگ الکترونیک |
| ۱۰ | ۰/۰٤۸ | فرماندهی |

### ٤-٣. رتبه‌بندی از منظر هزینه

استفاده از آسیب‌پذیری‌هایی چون شبکه و ارتباطات مانند ارتباطات ماهواره‌ای،... و همچنین فنّاوری و جنگ الکترونیک دارای بهترین رتبه و آسیب‌پذیری‌های فرماندهی مانند فرسایشی نمودن جنگ (شبکه فرماندهی کنترل) و افزایش بار اطلاعاتی همراه با عملیات روانی کمترین رتبه‌بندی هزینه را به خود اختصاص دادند. تفسیر آن این است که استفاده از آسیب‌پذیری‌هایی چون فرسایشی نمودن جنگ برای نیروی‌های مسلح ایران دارای هزینه‌های بسیار بالایی است.

جدول ۸: مقادیر وزنی آسیب‌پذیری‌ها از منظر هزینه

| نرخ ناسازگاری: ۰/۰۷<br>میزان وزن در آسیب‌پذیری: ۰/۲۸۷ | | |
|---|---|---|
| رتبه | مقادیر وزنی | آسیب‌پذیری |
| ۲ | ۰/۱۸۲ | فنّاوری |
| ٤ | ۰/۱۲٤ | علوم (پیچیدگی ...) |
| ۱ | ۰/۱۹۰ | شبکه و ارتباطات |
| ۵ | ۰/۰۸۳ | نیروی انسانی |
| ۹ | ۰/۰٤۸ | محیط جدید |
| ۸ | ۰/۰۵۵ | پردازش اطلاعات |
| ۷ | ۰/۰۵۹ | خطرات اطلاعات |
| ٦ | ۰/۰۷٤ | عملیات اطلاعاتی |
| ۳ | ۰/۱۵۷ | جنگ الکترونیک |
| ۱۰ | ۰/۰۲۸ | فرماندهی |

### ٤-٤. رتبه‌بندی از منظر اثربخشی

اثرگذارترین آسیب‌پذیری شامل پیشرفت علوم که شامل تئوری‌هایی چون علوم پیچیدگی، آشوب و تئوری سیستم است که منجر به مدل‌سازی رفتاری صحنه نبرد جنگ شبکه محور خواهد شد و همچنین فریب اطلاعاتی از رتبه‌های بعدی است. کم اثرترین آسیب‌پذیری ناشی از فنّاوری است. نکته حائر اهمیت آن است که آسیب‌هایی مؤثری چون علوم پیچیدگی از آسیب‌های ذاتی یک عملیات شبکه محور است. نیروهای مسلح ج.ا.ا برای استفاده از این نوع آسیب‌ها نیازمند هزینه بسیار بالا و زمان زیاد برای استفاده عملیاتی از این آسیب‌ها مواجه هستند.

جدول ۹: مقادیر وزنی آسیب‌پذیری‌ها از منظر اثربخشی

| نرخ ناسازگاری: ۰/۰۷<br>میزان وزن در آسیب‌پذیری: ۰/۲۳۷ | | |
|---|---|---|
| رتبه | مقادیر وزنی | آسیب‌پذیری |
| ۱۰ | ۰/۰٤٥ | فنّاوری |
| ۱ | ۰/۲۰۱ | علوم (پیچیدگی ...) |
| ۹ | ۰/۰٥٤ | شبکه و ارتباطات |
| ۸ | ۰/۰٥٥ | نیروی انسانی |
| ٥ | ۰/۰۸٥ | محیط جدید |
| ۳ | ۰/۱۲۹ | پردازش اطلاعات |
| ۷ | ۰/۰٦۲ | خطرات اطلاعات |
| ۲ | ۰/۱۸٤ | عملیات اطلاعاتی |
| ٦ | ۰/۰٦۳ | جنگ الکترونیک |
| ٤ | ۰/۱۲۰ | فرماندهی |

## ٥-٤. رتبه‌بندی از منظر امکان‌پذیری

ازلحاظ امکان‌پذیری نیز آسیب‌های فرماندهی، خطرات اطلاعاتی بیشترین رتبه‌بندی را به خود اختصاص دادند که با عملیات روانی و شناختی قابل حصول است و خطرات ناشی از فریب اطلاعاتی و پیشرفت علوم کمترین رتبه را به خود اختصاص دادند. هر چند استفاده از آسیب‌پذیری‌هایی چون فرماندهی نیاز به زمان و هزینه بسیار بالا می‌باشند.

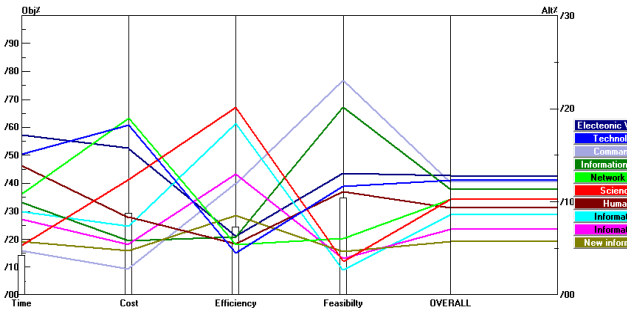
جدول ۱۰: مقادیر وزنی آسیب‌پذیری‌ها از منظر امکان‌پذیری

| نرخ ناسازگاری: ۰/۰٦<br>میزان وزن در آسیب‌پذیری: ۰/۳٤۰ | | |
|---|---|---|
| رتبه | مقادیر وزنی | آسیب‌پذیری |
| ٤ | ۰/۱۱٦ | فنّاوری |
| ۹ | ۰/۰۳۷ | علوم (پیچیدگی ...) |
| ٦ | ۰/۰٦۱ | شبکه و ارتباطات |
| ٥ | ۰/۱۱۱ | نیروی انسانی |
| ۷ | ۰/۰٤۷ | محیط جدید |
| ۸ | ۰/۰۳۹ | پردازش اطلاعات |
| ۲ | ۰/۲۰۱ | خطرات اطلاعات |
| ۱۰ | ۰/۰۲۷ | عملیات اطلاعاتی |
| ۳ | ۰/۱۳۱ | جنگ الکترونیک |
| ۱ | ۰/۲۳۱ | فرماندهی |

تمامی تحلیل‌ها و نتایج بر مبنای وزن شاخص‌های تصمیم‌گیری در پاییز ۹٦ بوده است. اگر در بازه زمانی مختلف اولویت و اهمیت این شاخص‌ها تغییر کند این مدل می‌بایست دوباره اجرا و تحلیل شود.

## ٦-٤. تحلیل حساسیت آسیب‌پذیری برمبنای معیارهای ارزیابی

با توجه به شکل (٥) ارزیابی حساسیت هر یک از آسیب‌پذیری‌ها با توجه به تغییرات وزنی شاخص‌ها مورد بررسی قرار گرفت.




شکل ٥: نمودار تحلیل حساسیت معیارهای آسیب‌پذیری

بر مبنای این تحلیل علاوه بر نرخ ناسازگاری که مؤید صحت نتایج است از تحلیل حساسیت نیز می‌توان چنین نتیجه‌ای دریافت نمود. در تحلیل حساسیت آسیب‌پذیری نسبت به زمان، موقعی‌که معیار زمان از وزن ۱۳/٦٪ به ۱۰۰٪ تغییر دهیم در آسیب‌پذیری‌های ارائه شده تغییری حاصل نشده است اما زمانی که وزن معیار زمان از ۱۳/٦٪ به سمت صفر میل کند و زمان ارزش کمتری به خود بگیرد آسیب‌پذیری فرماندهی گام‌به‌گام تغییر وضعیت و از رتبه‌های پایین به‌سرعت به رتبه‌های بالاتر تغییر وضعیت می‌دهد.

حساسیت آسیب‌پذیری‌ها نسبت به معیار هزینه، موقعی‌که مقدار وزنی هزینه رشد صعودی به ۱۰۰٪ را داشته باشد تغییری در سه آسیب‌پذیری فنّاوری، شبکه و جنگ الکترونیک که قبلاً دارای بیشترین آسیب‌پذیری داشتند ایجاد نخواهد شد اما اگر نیروی دفاعی کشور

مشکل جدی در هزینه نداشته باشد و اهمیت معیار وزنی به سمت صفر میل کند آسیب‌پذیری‌هایی چون فرماندهی، مخاطرات اطلاعات و جنگ الکترونیک دارای بیشترین رتبه‌بندی آسیب‌پذیری‌ها را به خود اختصاص خواهند داد.

اگر شاخص وزنی اثربخشی از مقدار تعیین شده تا مقدار وزنی ماکزیمم (۱۰۰٪) تغییر نموده رتبه‌بندی آسیب‌پذیری تغییری در رتبه‌بندی ایجاد نمی‌شود ولی زمانی مقدار وزنی اثربخشی نزولی و به سمت صفر میل کند آسیب‌پذیری‌های فنّاوری و جنگ الکترونیک دارای بیشترین رتبه خواهند شد.

زمانی که امکان‌پذیری به سمت اهمیت بسیار زیاد حرکت کند آسیب‌پذیری‌های فرماندهی و خطرات اطلاعاتی بیشترین رتبه را به خود اختصاص می‌دهند و وقتی‌که به سمت بسیار کم‌اهمیت میل کند آسیب‌پذیری‌هایی چون پیشرفت علوم، جنگ الکترونیک، فنّاوری دارای اهمیت و رتبه‌بندی بالاتری را به خود اختصاص می‌دهند.

## ۵. نتیجه‌گیری

برای پاسخ به سؤالات اصلی و فرعی پژوهش و ساخت مدل ارزیابی با توجه به شکل (۲) ارائه شد. سپس مراحل مدل‌سازی تشریح شده است. ابتدا ورودی‌های مدل که شامل آسیب‌پذیری‌های عملیات شبکه محور و معیارهای ارزیابی آسیب‌پذیری تعیین شد. آسیب‌پذیری‌های جنگ شبکه محور از منابع آشکار، جمع‌آوری دسته‌بندی‌شده است. کیفیت این دسته‌بندی آسیب‌پذیری در یک نشت اندیشه‌ورزی مورد تأیید قرار گرفت. با تشکیل پنلی از خبرگان نظامی، معیارهای ارزیابی آسیب‌پذیری‌ها با توجه به محیط پیچیده و پویا و در جهت استفاده مؤثر از آن‌ها به‌صورت معیارهای زمان، هزینه، اثربخشی و امکان‌پذیری مشخص شد. همچنین برای ارزیابی دقیق‌تر آسیب‌شناسی، زیرمعیارهای هر کدام به‌صورت زیر تعیین شد. برای معیار زمان؛ مدت زمان اجرا، پایداری زمانی، مدت زمان بهره‌برداری، مدت زمان بروزرسانی و زمان انقضا به‌عنوان زیرمعیارهای ارزیابی زمان ارائه شد. برای معیار هزینه، میزان هزینه لازم برای بهره‌برداری از آسیب‌پذیری، میزان هزینه برای عملیاتی‌شدن از آسیب‌پذیری به عنوان زیرمعیارهای ارزیابی هزینه مشخص گردید. برای ارزیابی معیار اثربخشی، میزان منافع حاصل از استفاده از آسیب‌پذیری و پیامدهای منفی حاصل از به‌کارگیری آسیب‌پذیری به‌عنوان زیرمعیارهای ارزیابی اثربخشی مشخص گردید. همچنین برای ارزیابی معیار امکان‌پذیری، میزان به‌کارگیری آسیب‌پذیری و تسهیل دستیابی به بهره‌برداری از آسیب‌پذیری به‌عنوان زیرمعیارهای ارزیابی امکان‌پذیری مشخص گردید. اعتبار این شاخص‌ها بر مبنای ضریب آلفای کرونباخ ۸۲٪ تعیین شده است. با توجه به معیارها و زیرمعیارها رتبه‌بندی آسیب‌پذیری‌ها با توجه به نظر خبرگان منتخب در بازه زمانی زمستان ۱۳۹۶ مشخص گردید. خروجی پیاده‌سازی مدل پیشنهادی شامل آسیب‌پذیری‌هایی چون جنگ الکترونیک، فنّاوری و آسیب‌پذیری از منظر فرماندهی از آسیب‌های جدی جنگ شبکه محور بوده است. همچنین نیروهای مسلح ج.ا.ا. می‌تواند برای هر یک از آسیب‌پذیری راه‌های استفاده و مدیریت آن‌ها درصحنه نبرد استراتژی مناسب اتخاذ کند. همچنین رتبه‌بندی آسیب‌پذیری‌ها از منظر زیرمعیارهای ارزیابی مورد بررسی و ارزیابی قرار گرفته است که خود شامل نتایج مهمی است که از جنبه‌های مختلف آسیب‌پذیری‌ها

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ۱، بهار ۱۳۹۷

را مورد تحلیل و ارزیابی قرار داده است. نرخ ناسازگاری به طور متوسط ۰/۰۷ است که معیاری برای صحت انجام این پژوهش است.

## ٦. پیشنهادها

با توجه به کاربردی بودن پژوهش پیشنهاد می‌گردد نیروی مسلح جمهوری اسلامی ایران با توجه به مدل مذکور در بازه‌های زمانی آتی آسیب‌پذیری‌های جدید را به این مدل اضافه و یا با توجه به شرایط جاری توانمندهای نیروهای مسلح ایران به مقایسه‌ها زوجی و ارزیابی و رتبه‌بندی آسیب‌پذیری‌ها اقدام شود. پس بر مبنای ارزیابی این آسیب‌پذیری‌ها می‌تواند نقشه راه کوتاه‌مدت، میان‌مدت و بلندمدت طراحی و اجرا نماید. پیشنهاد می‌شود در آینده و در بازه‌های زمانی مشخص با توجه به تغییر شرایط صحنه و قابلیت‌های نیروهای مسلح ایران، برمبنای مدل پیشنهادی این آسیب‌پذیری‌ها و همچنین شاخص‌های ارزیابی دوباره ارزیابی و در صورت نیاز بروزرسانی گردد. همچنین پیشنهاد می‌شود به صورت کاملاً تخصصی از این الگو برای ارزیابی آسیب‌پذیری‌ها در سطح نیروهای نظامی مانند دریایی، هوایی و زمینی به صورت مجزا استفاده و انجام شود.

از لحاظ دانشی پیشنهاد می‌گردد برای مقایسه و دقت بیشتر، این مدل‌سازی را با روش‌های دیگر تصمیم‌گیری چندمعیاره مانند تاپسیس و تحلیل شبکه‌ای با در نظر گرفتن وابستگی میان آسیب‌پذیری‌ها و شاخص‌های ارزیابی انجام شود.

همچنین پیشنهاد می‌گردد با توجه به عدم قطعیت خبرگان در ارائه داده‌های مناسب روش‌های تحلیل فرایند سلسله مراتبی فازی مورد ارزیابی قرار گیرد.

## ۷. مراجع


[1] US.DoD ،"Network Centric Warfare،" Department of Defense Report to Congress ،Wishington,DC ،2001.

[2] Tunnell.H ،"Task Force Stryker Network-Centric Operations in Afghanistan،" National Defense University Center for Technology and National Security Policy ، Washington, DC. ،2011.

[3] G. C. A. Byford ،"“Air Power Review:Network Enabled Capability, Air Power and Irregular Warfare: The Israeli Air ForceExperience in the Lebanonand Gaza,2006-2009،" تألیف Director Defence Studies (RAF) ،2010.

[4] McDermott ،"Russia Tests Network-Centric Air Operations in Syria،" Eurasia Daily Monitor Volume: 12 Issue: 184 ، 2015.

[5] R. McDermott ،"Russia’s Network-Centric Warfare Experiment in Syria،" Eurasia Daily Monitor Volume: 13 Issue: 76 ،2016.

[6] M. Vego ،"Operational Warfare،" 2003.

[7] M. J. H. Scherrer ،"Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity،" 2003.

[8] C. Wilson ،"Network Centric Warfare: Background and Oversight Issues for Congress،" CRS Report for Congress ، 2004.

[9] US.DOD ،"Net-Centric Environment Joint Functional Concept،" US Department of Defense ،Wishington,DC ،2005.

[10] J... J. G. a. F. P. S. Alberts.D ،Network Centric Warfare: Developing and leveraging information superiority ، Washington.DC: CCRP ،1999.

[11] .US.OFT ،"Network Centric Operations Conceptual Framework Version 1.0،" Evidence Based Research Inc ،2003.

[12] ع. فطانت. م. ن. فشارکی، "ارائه یک معماری مبتنی بر عامل بر پایه توافقات چند وجهی التزام برای شبیه‌سازی جنگ شبکه‌مدار،" چهارمین کنفرانس علمی فرماندهی و کنترل ایران، ۱۳۸۹.

[13] ج. ایزدی. ح. الماسیان. ع. شکیبامنش.، "بررسی مقایسه جنگ شبکه‌مدار و سیستم‌سیستم‌ها،" هفتمین کنفرانس علمی فرماندهی و کنترل، ۱۳۹۲.

[14] ع. شکیبا. ع.فطانت. م. فشارکی.، "کارگیری مدل‌های مرجع جی دی آل و سسا در توسعه مفهومی مرکز هوشمندانه دانش جنگ‌های شبکه مدار،" چهارمین کنفرانس علمی فرماندهی و کنترل ایران، ۱۳۸۹.

[15] م.فشارکی. ه. عطارن. حسین‌پرور، "طراحی مدل شیءگرای سیستم آگاهی اشتراکی وضعیت در تصمیم‌گیری شبکه مدار،" چهارمین کنفرانس علمی فرماندهی و کنترل ایران، ۱۳۸۹.

[16] M. J. H. Scherrer ،"Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity،" February 2003.

[17] S. French. G. ،"The Coming Counterrevolution in Military Affairs،" 2003.

[18] E. C. Blash ،"Network-Centric Warfare Requires a Closer Look،" May 2003.

[19] K. Rikhye.R ،"Analysis of Vulnerabilities Created by Us net-centric Warfare Introduction Until the First Gulf،" تألیف ITEC 610 ،2014.

[20] R. Giffin ،"Superstitious Rituals: Naïve Inductivism in Command and Control Doctrine: Its Causes, Consequences and Cures،" 2001.

[21] D. J. G. R. Reid ،"Network Centric Warfare and the Virtuous Revolution,،" 8th ICCRTS Symposium ،Washington ، 2003.

[22] Kaufman.A ،"Be careful what you wish for:The dangers of fighting with a network centric military،" Journal of Battlefield Technology ،pp. Vol 5, No 2 ،2002.

[23] Barnett ،"The Seven Deadly Sins of Network Centric Warfare،" 1999.

[24] Borgu. A ،"The Challenges and Limitations of "Network Centric Warfare" - The initial views of an NCW sceptic،" تألیف Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations Conference ،2003.

[25] U. Gangadharaiah ،"Network Centric warfare: A Survey،" International Journal of Computer Network and Wireless Communications(IJCNWC) ،2014.

[26] Kisling. ،"Analysis of Vulnerabilities Created by Us net-centric Warfare،" April 2014.

[27] A. D. Col. Campen ،"Look Closely At Network-Centric Warfare,،" USAF, Signal ،2001.

[28] B. P. D. R. Fowler ،"Induced Fragility in Information Age Warfare،" 1997.

[29] F. Kagan ،"War and Aftermath،" 2003.

[30] A. Litvaitis ،"Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment،" Baltic Security and Defence Review ،p. 143 to 170 ،2008.

[31] C. M. و. M. P.M ،"Human Supervisory Control Challenges in Network Centric Operations،" Massachusetts Institute of Technology ،2005.

[32] P. L. D. Houghton ،"21st Century Command, Comparison of Current Military Command Evolution and Potential Future Requirements،" 2001.

[33] J. Erbetta ،"Attrition in Network Centric Warfare،" تألیف published in RTO-MP-117 ، 2002.

[34] P. Forgues ،"Command in a Network-Centric War،" 2001.

[35] French.G ،"The Coming Counterrevolution in Military Affairs،" 2003.

[36] A. D. U. Col. Campen ،"Look Closely At Network-Centric Warfare،" 2004.

[37] J. D. C. Rosenburger ،"The Inherent Vulnerabilities of Technology: Insights from the National Training Center's Opposing Force،" US Army. ،2000.

[38] E. Blash ،"Network-Centric Warfare Requires a Closer Look،" May 2003.

[39] I. Kaufman A. ،"Be careful what you wish for:The dangers of fighting with a network centric military،" 2002.

[40] P. C. D. Houghton ،"JOCS/JCSI Information Case Study Report،" 1998.

[41] P. Houghton ،"Potential Vulnerabilities of a Network Enabled Force،" ۹th ICCRTS ، 2004.

[42] I. Coat ،"Use of Communications EW in a Network Centric Warfare Environment،" AOC International Exhibition and Symposium ،2008.

[43] S. T.L. ،"The analytic Hierarchy Process،" Mc Graw-Hill, New York ،1980.