فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال سوم، شماره یک، بهار ۱۳۹۸

توسعه مفهوم تهدید بر پایه تحمل‌پذیری و طراحی یک سیستم تصمیم‌یار برای ارزیابی میزان تهدید بر اساس گزاره‌های منطقی و شواهد گسسته مقدار در صحنه نبرد دریایی

سعید کاملیان[۱]، ناصر پریز[۲*]، علی کریم‌پور[۳]

تاریخ دریافت: ۱۳۹۷/۱۱/۰۵ تاریخ پذیرش: ۱۳۹۸/۰۳/۱۵

چکیده

تهدید یکی از کلیدی‌ترین معیارهای تصمیم‌گیری در صحنه عملیاتِ فرماندهی و کنترل دریایی است. پویایی بالا و محدودیت‌های زمانی که در طبیعت عملیات دریایی وجود دارد، فرآیند ارزیابی تهدید را برای اپراتوری که به واسطه انجام همزمان سایر اقدامات کنترلی استرس و بار ادراکی زیادی را تجربه می‌کند دشوار و پیچیده می‌نماید. از این رو فرآیند ارزیابی تهدید نیازمند به یک سیستم تصمیم‌یار است تا اپراتور را در دستیابی به نتایجی دقیق‌تر و با قابلیت اطمینان بیشتر یاری کند. فرآیند ارزیابی تهدید با تفکیک آن به ارکان پایه‌ای‌تر اعم از توانمندی، قصد و فرصت و سپس تولید شاخص‌هایی برای ارزیابی این مفاهیم تحقق می‌پذیرد اما در این پژوهش توسعه مفهومی ویژه‌ای برای تهدید پیشنهاد شده است. رکنی به نام تحمل‌پذیری به مجموعه ارکان تهدید اضافه شده و شاخص‌هایی برای ارزیابی آن ارائه شده است. همچنین برای امتیازدهی به پارامترهای اختصاصی هریک از ارکان تهدید یک رویکرد منطقی بدیع مبتنی بر شواهد گسسته-مقدار معرفی شده است. سپس یک سیستم تصمیم‌یار تمامی این شواهد را آنالیز می‌کند و براساس برآیند امتیازات پارامترها یک تابع امتیاز برای هریک از ارکان تهدید اختصاص خواهد داد. در نهایت یک آرایه چندبعدی که متشکل از بازه‌هایی از پیش تعیین شده برای ارکان تهدید است برای تعیین مقدار تهدید مورد استفاده قرار می‌گیرد. سپس مدل پیشنهادی برای ارزیابی تهدید در یک سناریوی دریایی مورد آزمایش قرار گرفته است. نتایج این آزمایشات حاکی از توانمندی این رویکرد در ارزیابی دقیق‌تر میزان تهدید است.

واژگان کلیدی: ارزیابی تهدید، سیستم تصمیم‌یار، شواهد گسسته مقدار، صحنه عملیات دریایی، گزاره‌های منطقی

[۱] دانشجوی دکتری مهندسی برق-کنترل، دانشکده مهندسی برق، دانشگاه فردوسی مشهد kamelian@mail.um.ac.ir

[۲] استاد گروه مهندسی برق-کنترل، دانشکده مهندسی، دانشگاه فردوسی مشهد n-pariz@um.ac.ir (نویسنده مسئول)

[۳] دانشیار گروه مهندسی برق-کنترل، دانشکده مهندسی، دانشگاه فردوسی karimpor@um.ac.ir

۱. کلیات

تهدید به معنای ساده عبارت است از قصد و نیت وارد آوردن آسیب و صدمه و یا اراده برای ایجاد تعارض زیان آور و آسیب زا [۱]. در سامانه‌های فرماندهی و کنترل دریایی و در فرآیندهای تحلیلی مربوط به آن ها، تصمیم‌گیران علاوه بر هدایت فعالیت‌های کنترلی ملزم به مدیریت تهدیدهایی هستند که متوجه ناوگان خودی می‌شود. به دلیل کیفی بودن ماهیت تهدید فرآیند آنالیز، ارزیابی و مدیریت آن توسط نیروهای خبره صورت می‌گیرد [۲, ۳]. هرچند که فرآیندهای سامانه‌های پایش و رهگیری اغلب خودکار دنبال می‌شود اما تصمیم‌گیری پیرامون تهدید به دلیل حساسیت و اهمیت بالایی که دارد می‌بایست توسط یک اپراتور خبره انجام شود و سپس توسط توابع دیگر سامانه‌های خودکار مورد استفاده قرار می‌گیرد[1]، چرا که نتایج ارزیابی تهدید نهایتاً برای صدور فرامین درگیری و استفاده از تسلیحات مورد استفاده قرار خواهد گرفت و هر نوع خطا در محاسبه و اولویت‌بندی تهدیدات و نسبت دادن تهدید بیشتر به اهدافی که تهدید محسوب نمی شوند و یا نسبت دادن تهدید کمتر به اهدافی با تهدید بالا منجبر به ایجاد نتایج غیرقابل جبرانی خواهد شد [٤-٦]. از سوی دیگر به دلایلی نظیر: پیچیدگی روزافزون محیط‌های عملیاتی، تعدد اهداف عملیاتی، تنوع در مأموریت‌ها و عدم قطعیت‌های بالا در فرآیند ارزیابی تهدید موجب می‌شود که فرآیند ارزیابی و مدیریت تهدید نیازمند به یک سیستم تصمیم‌یار باشد تا اپراتور را دستیابی به نتایجی دقیق‌تر و با قابلیت اطمینان بیشتر یاری کند.

۱-۱- بیان مسأله

موقعیت یک شناور خودی[2] را در پهنه دریا تصور کنید. حضور این شناور به عنوان یکی از بازیگران اصلی حاضر در صحنه به همراه موجودیت[3]های دیگری که در ارتباط با او قرار می‌گیرند منجر به شکل‌گیری یک موقعیت تاکتیکی[4] خواهد شد [۷]. چنانچه احتمال متخاصم بودن موجودیت‌های حاضر در صحنه قابل توجه باشد یک موقعیت تهدیدی[5] شکل خواهد گرفت. موقعیت تهدیدی به معنای این است که یک عامل تهدید کننده[6] در پی انجام یک اقدام تهدید آمیز خودآگاه علیه یک عامل تهدید شونده[7] است. این اقدام تهدید آمیز که منجر به صدمه یا خسارت برای عامل تهدید شونده است، حمله[8] نامیده می‌شود.

مسأله ارزیابی تهدید عبارت از اختصاص یافتن یک مقدار $TA_{ij} \in [0.1]$ به هر زوج مرتب $(T_i.A_j)$ که بیانگر میزان تهدید (TA_{ij}) هر عامل تهدیدکننده T_i برای هر دارایی[9] خودی A_j و سپس اولویت‌بندی کردن عوامل تهدیدکننده بر اساس میزان تهدید است. ارزیابی تهدید شامل مجموعه‌ای از توابع است که خروجی نهایی آن‌ها منجر به ارتقاء آگاهی وضعیتی تصمیم‌گیران شده و بار ادراکی آن‌ها را کاهش می‌دهد.

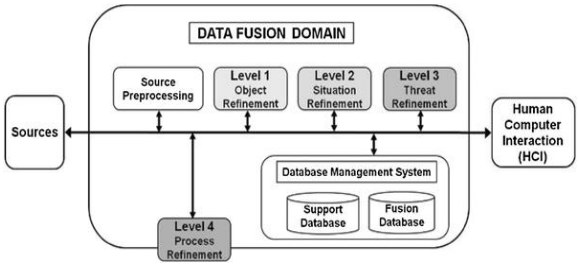
۱-۲- اهمیت و ضرورت طرح

ارزیابی تهدید به صورت ذاتی شامل استدلال کردن پیرامون برهمکنش‌ها، اثرات متقابل و سایر ارتباطات میان موجودیت‌های حاضر در صحنه است. تقابل‌های شکل گرفته پیرامون منافع، موقعیت‌ها، پیشرفت‌ها، دستاوردها و جایگاه‌ها در بستر زمان و محدودیتی که از حیث وجودی در کسب آن‌ها وجود دارد منجر به شکل‌گیری تهدید می‌شود. بر این اساس تهدید می‌تواند به صورت روابط بالقوه و بالفعل میان موجودیت‌هایی که تهدید آمیز هستند و موجودیت‌هایی که در معرض تهدید هستند مدل شود [۸]. مفاهیم کلیدی‌تر تهدید که سازنده پایه‌های یک رویداد تهدیدی هستند در [۸-۱۱] آمده است. اما تهدید در مدل تلفیق داده با عنوان کلی‌تر ارزیابی اثر یا ضربه[10] مورد توجه قرار گرفته است. همانطور که در شکل (۱) دیده می‌شود ارزیابی اثر در مدل **JDL** تلفیق داده در سطح سه انجام می‌شود [۱۲-۱٤]. در تعریف **JDL** ارزیابی اثر، به فرآیند پیش‌بینی و تخمین اثراتی که توسط موجودیت‌های یک محیط عملیاتی بر موقعیت‌ها،

[1] Man in Loop
[2] Ownship
[3] Entity
[4] Tactical situation
[5] Threatening situation
[6] Threatening agent
[7] Threatened agent
[8] Attack
[9] Asset
[10] Impact assessment

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال سوم، شمارهٔ یک، بهار ۱۳۹۸

روابط، کنش‌ها و منافع طرفین وارد می‌شود اطلاق شده است [۱۵].



شکل (۱) : مدل JDL برای تلفیق داده و جایگاه ارزیابی تهدید [۱۴]

ارزیابی اثر شامل برهمکنش‌های میان برنامه‌ها و اهداف عملیاتی بازیگران مختلفی است که در صحنه عملیات حضور دارند [۱۵]. برنامه عملیاتی در حقیقت شامل زنجیره‌ای از اقدامات مرتبط است که توسط یک بازیگر در محیط عملیاتی به وقوع می‌پیوندد. هر اقدام به طور ذاتی اثرات و تبعاتی را ایجاد می‌کند که محیط عملیات را تحت تأثیر قرار داده و موقعیت‌های آن را دچار تغییر می‌کند. این اثرات ممکن است با اقدام اولیه همزمان باشند و یا نباشند. اثر مربوط به هر اقدام هرچه که باشد می‌تواند تأثیرات قابل توجهی بر برنامه عملیاتی بازیگران دیگر داشته باشد و آن‌ها را ناچار به تغییر برنامه عملیاتی کند به نحوی که برخی از اقدامات برنامه ریزی شده خود را لغو کرده و اقدامات دیگری را جایگزین آن کنند. ارزیابی اثر در مدل **JDL** مقدمه تحلیل تهدید است. اما چه معیار و شاخصی است که نوع اقدام و اولویت آن را تعیین می‌کند؟

همانطور که پیش‌تر اشاره شد یک موجودیت با قرارگرفتن در یک موقعیت تاکتیکی برنامه عملیاتی خاص خود را به اجراء خواهد گذاشت. اما وقوع رخدادهای تهدیدی و یا پیشبینی آن‌ها توسط هر موجودیت می‌تواند این برنامه عملیاتی را دستخوش تغییر کند. بنابراین برای داشتن یک برنامه عملیاتی بروز و کارآمد لازم است که هر موجودیتی به طور مداوم به ارزیابی و تخمین تهدیدات در موقعیت تاکتیکی خود بپردازد تا زنجیره اقداماتش را در راستای کاهش تهدید و یا به حداقل رساندن آسیب‌های ناشی از رخدادهای تهدیدآمیز طرح ریزی کند. از این رو ارزیابی تهدید نیازمند طراحی یک فرآیند محاسباتی است که کلیدی‌ترین بخش این فرآیند کمی سازی مفهوم تهدید و به عبارت بهتر محاسبه تهدید برای هر موجودیت و بازیگر حاضر در صحنه عملیات است. این فرآیند را می‌توان با رویکردهای مختلفی به انجام رساند که در ادامه به برخی از روش‌های توسعه یافته برای آن اشاره خواهیم کرد و رویکرد ابداعی این پژوهش در انتها مطرح خواهد شد.

این پژوهش به صورت زیر تنظیم شده است. در بخش دو پیشینه پژوهش مورد بررسی قرار گرفته و رویکردهای مختلف در ارزیابی و کمی‌سازی تهدید اشاره شده است. بخش سه به تشریح و بررسی رویکرد این پژوهش در توسعه مفهومی تهدید می‌پردازد و تحمل‌پذیری به عنوان رکن جدیدی برای ارزیابی تهدید معرفی شده و شاخص‌هایی برای آنالیز آن ارائه می‌شود. سپس مشخصات سیستم تصمیم یاری که بر مبنای گزاره‌های منطقی و شواهد گسسته مقدار کار می‌کند ارائه شده است. بخش چهارم به بیان نتایج و دستاوردهای پژوهش اختصاص دارد وموفقیت مدل پیشنهادی در ارزیابی تهدید در مقایسه با سایر روش‌های موجود مورد اشاره قرار گرفته است. در نهایت در بخش پنجم به جمع‌بندی نکات پرداخته شده و مسیرهایی برای پژوهش‌های آتی ترسیم شده است.

۲. ادبیات پژوهش

پیش از توسعه روش ها، سیستم‌ها و الگوهای تصمیم یار[1]، سنجش میزان تهدید یک موجودیت در صحنه عملیات عمدتاً توسط انسان صورت می‌پذیرفت. اما با تغییر ماهیت‌ها و خصوصیات محیط‌های عملیاتی به ویژه در حوزه‌های نظامی که حاکی که از بهره‌گیری هرچه بیشتر از توان ماشین‌های محساباتی دارد، فضا برای انتقال و برون سپاری برخی از وظایفی که پیش‌تر توسط انسان انجام می‌شد به ماشین‌ها آماده شد. از این رو بسیاری از کارکردهای اپراتورهای خبره به ماشین‌ها سپرده شد و توابع هوشمند و سیستم‌های پردازشی قدرتمندی برای پیشبرد این موضوع آفریده شد. سیستم‌های تصمیم‌یار در حالی که همچنان زنجیره نهایی فرماندهی و کنترل را برعهده **ندارند** به ارتقاء آگاهی محیطی و کاهش عدم قطعیت‌ها به کاربران خود کمک می‌کنند. در فرآیند برون سپاری وظایف محاساباتی و

[1] Decision support system - DSS

تحلیلی اپراتورها به ماشین، ارزیابی تهدید به دلایل زیر یکی از چالش برانگیزترین آن‌ها محسوب می‌شود:

- تهدید یک مفهوم کمی است که در نگاه اول برای ماشین قابل تبیین نخواهد بود [۱۵].
- تهدید یک حقیقت پیوسته-پویاست[1] که طبیعت و ماهیت آن تا حدودی متغیر است [۹, ۱۶].
- تهدید می‌تواند از شکل یک تمامیت یکپارچه واحد[2] به شکل یک تمامیت متفرق[3] تغییر حالت دهد [۹].
- تهدید کلیدی‌ترین عنصر تصمیم‌گیری در یک صحنه عملیات نظامی است چرا که پایه و نقطه شروع تولید اقدامات لازم برای مقابله با تهدید و تصمیم‌گیری نهایی پیرامون اجرای آن‌هاست [۱, ۱۷].

۲-۱. پیشینه شناسی

مطابق با آنچه در [۱۵] آمده است، محاسبه تهدید می‌تواند با نگاه به گذشته، حال و آینده اقداماتِ موجودیت‌های حاضر در صحنه عملیات آغاز شود. این نگاه به منظور شناسایی موقعیت‌های خطر آفرین[4] انجام می‌پذیرد و میزان اثرگذاری این موقعیت‌ها بر اهداف مأموریت، برنامه و طرح اقدامات، نیروی انسانی، دارایی‌های ارزشمند و سایر مراکز ارزش سنجیده می‌شود. در نهایت هر موجودیت و بازیگری در صحنه عملیات که شناسایی شده باشد با عناوینی چون: دشمن، دوست، خنثی برچسب گذاری خواهد شد. در این رویکرد برای محاسبه کمی تهدید لازم است تا آنالیزهای مفصلی بر روی محیط عملیات، انگیزه بازیگران و توانایی‌های آن ها، شرایط زمانی – مکانی[5] موقعیت‌ها انجام شود. شبکه‌ای از آنالیزهای مرتبط که برای محاسبه تهدید مورد نیاز است در [۱۵] ذکر شده است.

در [۱] تشریح دقیقی از یک فرآیند محاسبه تهدید ارائه شده است. این فرآیند بر اساس شناسایی و دسته بندی پارامترهایی که در ادبیات موضوعی برای محسابه مقدار تهدید ارائه شده، آغاز شده است. سپس پارامترهای مفروض به صورت رئوس یک گراف جهتدار در نظر گرفته شده‌اند و ارتباط میان آن‌ها از با استفاده از یال‌های گراف مشخص شده است. پس از اینکه ساختار شبکه بیزی پیشنهادی بر اساس فاکتورهای مؤثر در محاسبه تهدید و ارتباط آن‌ها تکمیل شد، توابع توزیع احتمال خلاقانه‌ای برای هر پارامتر پیشنهاد شده و یک جدول از مقادیر احتمال شرطی تولید می‌شود. میزان تهدید هر موجودیت با آنالیز مقادیر این جدول و قرارگرفتن آن‌ها در ساختار شبکه بیزی تعیین شده و پیرامون آن تصمیم‌گیری می‌شود. استفاده از شبکه‌های بیزی برای ارزیابی تهدید در [۱۸-۲۳] نیز مورد توجه قرار گرفته است.

ارزیابی تهدید بر اساس قواعد از پیش تعیین شده، یکی دیگر از رویکردهای کلاسیک در موضوع تهدید است. در این روش‌ها مجموعه از الگوهای ذهنی برای شناسایی و ارزیابی میزان تهدید طراحی می‌شود. الگوهای طراحی شده سپس در قالب قواعدی زبانی[6] ارائه می‌شوند. قواعد زبانی آماده شده در پتلفورم‌های زبانی پیاده شده و برای ارزیابی کمیت مورد نظر بکار گرفته می‌شوند [۲۴-۲۶].

محاسبه مقدار تهدید از طریق کمی سازی ارکان کلیدی آن یعنی: انگیزه یا قصد، توانمندی و فرصت در [۸, ۱۱, ۲۷] انجام شده است. در این رویکرد با در نظر گرفتن مجموعه‌ای از آنالیزهای مفصل برای ارزیابی ارکان تهدید، یک فرآیند بسیار خلاقانه برای پیش‌بینی میزان تهدید پیشنهاد شده است. در این فرآیند از آنالیست‌های خبره خواسته شده است که میزانی برای احتمال و میزانی برای ضریب وزنی اثر گذاری هر المان تهدید پیشنهاد دهند. این احتمالات و ضریب‌های اثر گذاری با استفاده از از مدل‌های پیش‌بینی که بر اساس سوابق تاریخی و آماری و یا مدل‌های تحلیلی شکل گرفته‌اند تولید می‌شود.

استفاده از اطلاعات و نتایج رهگیری رویکردی است که در [۲۸] برای ارزیابی تهدید مورد استفاده قرار گرفته است. در این رویکرد با استفاده از تکنیکی موسوم به استخراج رفتار هدف[7] از روی داده‌های سنسوری که در [۲۹] به تفضیل شرح داده شده ،

[1] Continuant dynamic
[2] Unit whole
[3] Disperse whole
[4] Menacing situations
[5] Spatio-temporal
[6] Linguistic rules
[7] extracting target behaviors

روشی برای محاسبه تهدید اهداف هوایی ارائه شده است. در این رویکرد شاخص‌هایی برای کمی سازی و محاسبه قصد و توانمندی اهداف بر مبنای اطلاعات به دست آمده از رهگیری ارائه شده است. این شاخص‌ها از نوع زمان – مکانی هستند و با استفاده از گزاره‌های منطقی که خروجی آنها به شکل صفر یا یک است تبیین می‌شوند. درنهایت مجموع وزن‌دار نرمالیزه شده شاخص‌ها برای ارزیابی تهدید مورد استفاده قرار خواهد گرفت. قواعد استنتاج فازی نیز به طور گسترده‌ای برای محاسبه سطح تهدید اهداف حاضر در صحنه عملیات مورد استفاده قرار گرفته است [۲۰, ۳۰-۳۶]. در این رویکرد برای هر پارامتر مرتبط با تهدید سه تابع عضویت کم، متوسط و زیاد در نظر گرفته شده است. این توابع عضویت، هر نقطه‌ای در فضای ورودی را به مقدار عضویتی میان صفر و یک می‌نگارند. سپس از طریق یک موتور استنتاج فازی مقادیر ارزیابی شده و میزان تهدیدها برای هریک از موجودیت‌ها تعیین می‌شود.

دسته‌ای دیگر از الگوریتم‌ها برای ارزیابی میزان تهدید روش‌های مبتنی بر الگوهای از پیش تعیین شده قبلی هستند [۵, ۳۷]. در این رویکرد پس از کشف اهداف، فرآیند ارزیابی تهدید توسط اپراتور آغاز می‌شود. او با فعال کردن یک الگوی مشخص، متناسب با نوع هدف شناسایی شده میزانی از تهدید را به این هدف نسبت می‌دهد. فرآیند با ارزیابی پارامترهای مرتبط با تهدید توسط ماشین ادامه می‌یابد. ماشین پارامترهای مرتبط با تهدید را برای هدف شناسایی شده اندازه‌گیری کرده و ارزیابی می‌کند و سپس مقدار این پارامترها را پارامترهای الگوی تعیین شده توسط اپراتور و میزان تهدید اولیه مقایسه می‌کند. بر اساس میزان تطبیق پارامترهای واقعی با پارامترهای الگو میزان تهدید کم یا زیاد خواهد شد. در [۳] ابزاری برای تصمیم‌گیری پیرامون تهدید ارائه شده است که بر اساس مجموعه‌ای از تحلیل‌های در یک فرآیند شبکه‌ای[1] کار می‌کند. معیارهای که دارای ارتباط هستند در یک شبکه سلسله مراتبی تحلیل می‌شوند و در انتها تهدیدی یا غیر تهدیدی بودن آن‌ها تعیین می‌شود.

بررسی و ارزیابی تهدید ناشی از بکارگیری سنسورها و تجهیزات اندازه گیری از موضوعاتی است که کم‌تر بدان پرداخته شده است. در [۳۸] برای ارتقاء کارایی سامانه جمیمنگ فرآیندی برای ارزیابی میزان تهدید شبکه‌های راداری پیشنهاد شده است. بهینه سازی عملکرد سامانه‌های جمینگ بر اساس شاخص‌های تهدید و ارزیابی آن‌ها صورت می‌گیرد.

استفاده از انواع شبکه‌های عصبی در تحلیل میزان تهدید یکی دیگر از رویکردهایی است که در پژوهش‌ها پی‌گرفته شده است. این روش‌ها تلفیقی از رویکردهای مدل محور و داده محور هستند که قابلیت بالایی در تحلیل سریع و دقیق تهدید دارند [۳۹-۴۲].

در [۴۳] تهدید به صورت شبکه‌ای از موجودیت‌ها و روابط میان آن‌ها مدل شده است. همچنین عدم قطعیت‌های موجود در روابط میان موجودیت‌ها به شکل توابع یقینی در حوزه تئوری شهود در نظر گرفته شده است. میزان تهدید بر اساس شواهدی که از رفتار اهداف استنباط می‌شود محاسبه شده و مورد ارزیابی قرار می‌گیرد.

علاوه بر پژوهش‌هایی که ارزیابی و تخمین تهدید را به شکل کلی و عام پی‌گرفته‌اند، مواردی نیز وجود دارند که در شرایط و محیط‌های خاصی به تحلیل و سنجش تهدید پرداخته‌اند. ارزیابی تهدید برای شناورهای دریایی در رویارویی با تهدیدات هوایی در [۲, ۶] مورد توجه قرار گرفته است. همچنین ارزیابی تهدید هوایی از دید مشاهده‌گر زمینی در [۴۴] بررسی شده است. ارزیابی تهدید برای تولید یک برنامه آتش[2] در [۴۵] مورد اشاره قرار گرفته است که در آن مجموعه‌ای از تسلیحات برای بکارگیری در برابر اهداف زمینی متعدد بر اساس میزان تهدید برنامه‌ریزی شده‌اند. همچنین ارزیابی تهدید با رویکرد مدیریت استراتژیک در [۴۶] دنبال شده است. در این رویکرد، ارزیابی تهدیدات نامتقارن با استفاده از مدل‌های تحلیلی هوشمند و بر اساس تئوری تداخل صورت پذیرفته است.

رویکرد این پژوهش در ارزیابی تهدید مبتنی بر شواهدی است که ارکان تشکیل دهنده تهدید را آنالیز می‌کنند. ارکان شناخته شده تهدید یعنی قصد، توانمندی و فرصت در پژوهش‌های مختلف بکار گرفته شده‌اند. اما تحمل‌پذیری به عنوان رکن چهارم ارزیابی تهدید در این پژوهش پیشنهاد شده است. افزودن

[1] Analytic network process - ANP

[2] Fire plan

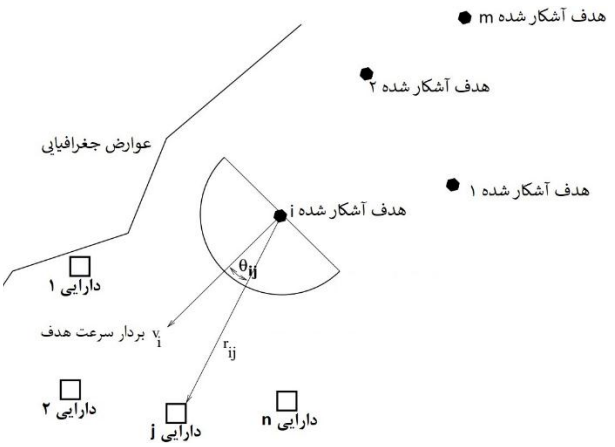
تحمل‌پذیری به ارکان تهدید زوایای دیگری از حقیقت تهدید را آشکار می‌کند که پیش از این وجود نداشته است. قرار گرفتن تحلیل‌های مربوط به تحمل‌پذیری در کنار تحلیل‌های سایر ارکان تهدید می‌تواند نتایج ارزیابی تهدید را به طرز قابل توجهی تغییر دهد و اولویت‌بندی تهدیدات با در نظر گرفتن تحمل‌پذیری دستخوش تغییرات اساسی خواهد شد. در ادامه برای هریک از ارکان تهدید شواهدی گردآوری و ارائه شده است. این شواهد در قالب گزاره‌هایی منطقی طرح شده‌اند و می‌توانند مقادیری گسسته اختیار کنند. اختصاص مقدار به این شواهد بسیار ساده صورت می‌پذیرد که کاهش بار محاسباتی و ادراکی اپراتور را به همراه دارد و چالاکی او را در ارزیابی تهدیدات افزایش می‌دهد. از سوی دیگر تعدد و تنوع شواهد موجب می‌شود تا آنالیز ارکان تهدید با غنای مناسبی انجام شود. سپس ارکان تهدید برای اختصاص مقداری به تهدید مورد استفاده قرار می‌گیرند. در بخش بعد به تشریح روش پیشنهادی خواهیم پرداخت.

۳. توسعه مفهوم تهدید بر پایه تحمل‌پذیری

۳-۱. هندسه موقعیت تاکتیکی

یک صحنه عملیات تاکتیکی را در نظر بگیرید. موجودیت‌هایی که در صحنه عملیات حاضر هستند شامل مجموعه دارایی‌هایی است که باید از آن‌ها محافظت شود. این مجموعه شامل تمامی مایملکی هستند که در پی مراقبت و صیانت از آن‌ها هستیم. این مجموعه به صورت $\mathrm{A}=\{A_1,\ldots,A_n\}$ نشان داده می‌شود. اهداف[1] دیگر موجودیت‌هایی هستند که در صحنه عملیات حضور دارند. منظور از اهداف در اینجا تمامی موجودیت‌هایی هستند که در محیط عملیاتی مطلوب کشف و آشکار شده‌اند. مجموعه اهداف نیز به صورت $\mathrm{T}=\{T_1,\ldots,T_m\}$ نشان داده می‌شوند. مسأله‌ای که لازم است بدان پرداخته شود این است که برای هر زوج مرتب (T_i,A_j) که در آن $A_j\in\mathrm{A}$ و $T_i\in\mathrm{T}$ است مقداری از تهدید اختصاص داده شود که نشان دهنده میزان تهدیدی است که از سوی هدف T_i متوجه دارایی A_j می‌شود.

فرآیند اختصاص دادن یک مقدار عددی به هر زوج مرتب (T_i,A_j) که نمایش دهنده میزان تهدید اعمالی از سوی هدف T_i به دارایی A_j است نیازمند تعریف یک تابع با عنوان تابع تهدید است. تابع تهدید $\mathrm{f}:\mathrm{T}\times\mathrm{A}\rightarrow[0,1]$ تابعی است که به هر زوج مرتب اشاره شده مقداری مابین صفر (به معنای فاقد تهدید) تا یک (به معنای حداکثر تهدید) نسبت می‌دهد. برای ارزیابی میزان تهدیدی که توسط هر هدف متوجه دارایی می‌شود، لازم است تا پارامترهایی که میزان یا مقدار تهدید را کنترل می‌کنند شناسایی کنیم. برای درک بهتر پارامترهایی که در ادامه مطرح خواهد شد بهتر است تصویر شماتیک شکل (۲) را در نظر داشته باشیم. در این تصویر هندسه مسأله و موقعیت یکی از اهداف و همچنین موقعیت دارایی‌هایی که در پی حفاظت از آن‌ها هستیم، دیده می‌شود.



شکل (۲) : هندسه مسأله و موقعیت یکی از اهداف و همچنین موقعیت دارایی ها

۳-۲. ساختار تهدید و ارکان تشکیل دهنده آن

برای درک بهتر مفهوم تهدید لازم است تا با مفاهیم تشکیل دهنده آن از جمله: قصد[2]، توانایی[3] و فرصت[4] آشنا شویم.

قصد یا انگیزه یکی از فاکتورهایی است که در مدلسازی تهدید مورد استفاده قرار می‌گیرد. بر این اساس قصد به معنای تصمیم‌گیری برای انجام یک کنش به شیوه‌ای خاص است. برای یک قصد مشخص شده، برنامه‌ای ویژه از اقدامات نیاز است تا

[1] Targets

[2] Intent
[3] Capability
[4] Opportunity

بتوان به هدف تعیین شده دست یافت. این برنامه ویژه همان پلن یا برنامه عملیاتی است. قصد در نگاه هستی شناسی و فلسفی، اراده یک بازیگر است که در پس این اراده مطلوبیت‌ها و علاقه‌مندی‌های مشخصی وجود دارد. مطلوبیت در این نگاه شامل تحریک‌های خودآگاهی است که بازیگر را به سمت اقداماتی سوق می‌دهد که دستیابی به نتایج این اقدامات رضایت، منفعت و لذت بیشتری را برای او به همراه خواهد آورد[1] [۹]. وجود مطلوبیت برای شکل‌گیری اقدام به تنهایی کافی نیست. علاوه بر مطلوبیت که منجر به شکل‌گیری قصد می‌شود توانمندی برای انجام اقدام نیز لازم است. به عبارت بهتر بازیگر باید پتانسیل و امکانات لازم را داشته باشد تا با استفاده از پتانسیل خود و بکارگیری امکاناتی که در اختیار اوست بتواند اقدام لازم را انجام دهد. در نهایت بازیگر باید فرصت انجام اقدام لازم را داشته باشد و این به معنای این است که مجموعه‌ای از شرایط و قیود باید وجود داشته باشند تا اقدام مورد نظر به نتیجه مورد انتظار خود برسد [۱۵]. در نهایت چنانچه قصد، توانمندی و فرصت برای یک بازیگر فراهم شود، او دست به اقدام خواهد زد به این معنا که مجموعه‌ای از اقدامات را برای رسیدن به اهداف خاصی در پیش خواهد گرفت. بنابراین برای شکل‌گیری مفهوم تهدید سه پایه اساسی لازم است [۹]:

- یک بازیگر در صحنه عملیات قصد آگاهانه برای انجام اقدامات تهدید آمیز داشته باشد.
- بازیگر مورد نظر باید قابلیت و توانمندی‌های لازم برای انجام اقدامات تهدید آمیز را داشته باشد.
- صحنه عملیات باید فرصت (شرایط و قیود) لازم برای به نتیجه رسیدن اقدام تهدید آمیز را فراهم کند.

۳-۳. تحمل‌پذیری و ارتباط آن با تهدید

ارزیابی تهدید تنها بر اساس سه رکن اشاره شده تمامی حقیقت تهدید را پوشش نمی دهد. چنانچه یک بازیگر در صحنه عملیات واقع شود و در یک موقعیت تاکتیکی که نیازمند تصمیم‌گیری است قرار گیرد، لازم است تا برای کسب آگاهی وضعیتی بالاتر و ارزیابی تهدید دقیق تر، به بررسی شرایط محیطی و رخدادهای صحنه عملیات بپردازد. اگر رخدادها و شرایط محیطی که متأثر از اقدامات سایر بازیگران حاضر در موقعیت تاکتیکی هستند تهدیدآمیز باشند، بازیگر مورد نظر باید میزان تحمل‌پذیری خود را در برابر اقدام تهدید آمیزِ رخداده (یا پیش‌بینی شده) برآورد کند تا بتواند برنامه عملیاتی خود را متناسب با آن بروز کرده و اقدام متقابل را انجام دهد. همچنین یک بازیگر میزان آسیب‌پذیری[2] خود را در صورت اجرای اقدام خودی در نظر می‌گیرد. این به معنای آن است که بازیگر در صورت انجام اقدامی که در برنامه عملیاتی اش گنجانده شده است، تا چه میزان در معرض آسیب فیزیکی، از دست رفتن منابع، صدمه و یا حمله متقابل قرار خواهد گرفت. آسیب پذیری یا میزان در معرض بودن ارتباط عمیقی با مفهوم تحمل‌پذیری[3] دارد. بازیگر باید قادر به تحمل تبعات و اثرات اقدام تهدید آمیز خود باشد، چرا که اقدام تهدید آمیزی که توسط یک بازیگر در محیط عملیاتی رخ می‌دهد طبق آنچه گفته شد منتج به اثراتی در محیط شده و سایر بازیگران حاضر در صحنه عملیات را وادار خواهد کرد که برنامه عملیاتی خود را متناسب با شرایط جدید بروزرسانی کنند. این بروزرسانی می‌تواند شامل حذف و لغو مجموعه‌ای از اقدامات و جایگزینی مجموعه‌ای دیگر به جای آن‌ها باشد و در این میان ممکن است بازیگرانی برنامه عملیاتی برای پاسخ به اقدام تهدید آمیز بازیگر اول داشته باشند. ارزیابی آسیب پذیری متقابل هر اقدام تهدید آمیز برای بازیگری که قصد اجرای این اقدام را دارد انگیزه و قصد بازیگر را تحت تأثیر قرار خواهد داد. به این معنا که چنانچه بازیگری با توجه به مطلوبیت‌ها و اهداف مد نظر خود قصد، توانمندی و فرصت انجام یک اقدام تهدید آمیز را داشته باشد اما قادر به تحمل شرایط و اثرات ناشی از این اقدام نباشد نمی تواند این اقدام را

[1] این نقطه شروع فرآیند است به این معنا که یک بازیگر در طلب دستیابی به چیزی است. زمانی که این نقطه آغازین با اراده بازیگر همراه شود قصد متولد می‌شود. اما پرسشی که باید به آن پاسخ داد این است که چطور می‌توان قصد یا نیت یک بازیگر را در صحنه عملیات شناسایی کرد. به عبارت بهتر پایش چه کمیتی می‌تواند به تعیین قصد بازیگر برای انجام یک (مجموعه) اقدام خاص منجر شود.

[2] Vulnerability

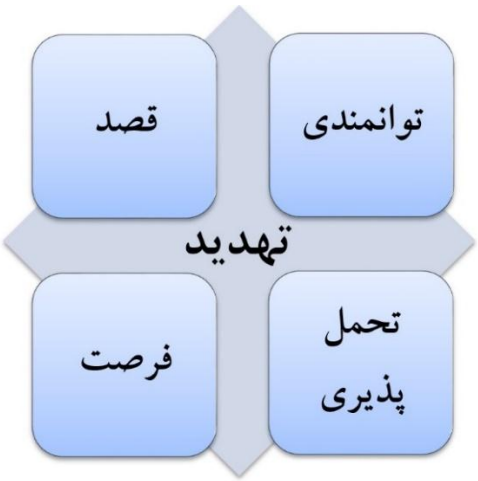
[3] Tolerability

انجام دهد. بنابراین تحلیلی که یک بازیگر از میزان آسیب پذیری خود و یا میزان تحمل‌پذیری خود دارد قصد و انگیزه او را برای انجام اقدام تهدید آمیز تحت تأثیر قرار خواهد داد.

ارزیابی تحمل‌پذیری به این معناست که هر بازیگر با توجه به موقعیت تاکتیکی که در آن قرار گرفته شروع به مشاهده رخدادها و شرایط محیطی می‌کند. این بازیگر برای ارزیابی میزان تهدیدِ موجودیت‌هایی که در پیرامون او هستند و به شکل مداوم بر محیط عملیاتی اثر می‌گذارند لازم است تا تحمل‌پذیری خود نسبت به این رویدادها را تحلیل کند. او اساساً برای اینکه رخداد و یا شرایطی را تهدید کننده قلمداد کند لازم است تا منشأ و مبدأ این رخداد و شرایط را در نظر بگیرد و سپس برای سنجش میزان تحمل‌پذیری خود موارد زیر را تحلیل کند.

- انجام یک اقدام تهدید آمیز مشخص برای مبدأ و منشأ آن اقدام چه هزینه‌ای دارد؟
- انجام یک اقدام تهدید آمیز مشخص برای مبدأ و منشأ آن اقدام چه دستاوردی دارد؟
- آیا دفاع یا اقدام متقابل برای غلبه بر اقدام تهدید آمیز رخداده اساساً ممکن است و اگر هست چه هزینه‌ای برای دفاع کننده دارد؟
- دفاع و اقدام متقابل در برابر رخداد تهدید آمیز چه دستاوری برای دفاع کننده دارد؟

با توجه به موارد ذکر شده چنانچه تهدید را به صورت یک حقیقت یکپارچه در نظر بگیریم این حقیقت مطابق شکل (۳) چهار جانبه[1] خواهد بود.



شکل (۳) : پایه‌های شکل‌گیری مفهوم تهدید

۳-٤. ارائه شواهد منطقی جهت تحلیل و امتیازدهی ارکان تهدید

تحقق ارزیابی تهدید برای هر موجودیت نیازمند آنالیز دقیق ارکان تهدید برای هر عامل تهدید کننده است. ما در این جا برای آنالیز ارکان تهدید از مجموعه‌ای از شواهد و گزاره‌های منطقی بهره جسته‌ایم. هر یک از ارکان تهدید می‌تواند با اسناد به شواهدی که در ادامه به تفضیل خواهد آمد مورد تحلیل قرار گرفته و مقدار دهی شود.

۳-٤-۱. شواهد ارزیاب قصد

از مهمترین شاخص‌هایی که برای تعیین میزان تهدید اهداف در صحنه عملیات به کار برده می‌شوند، پارامترهای کلاس قصد هستند. این پارامترها شامل طیف وسیعی از معیارهایی می‌شوند که حاوی شواهدی پیرامون قصد و انگیزه اهداف در صحنه نبرد هستند. این پارامترها به نوعی ارزیابی کننده مقاصد اهداف در صحنه عملیات هستند.

۳-٤-۱-۱. شواهد مجاورتی[2]

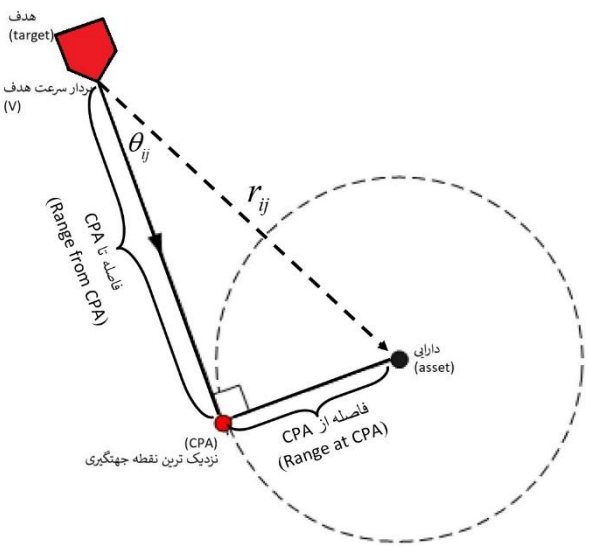
دسته مهمی از پارامترهایی که برای نسبت دادن مقدار تهدید به زوج مرتب هدف دارایی مورد استفاده قرار می‌گیرند پارامترهای کلاس مجاورت[3] هستند. این پارامترها سنجشی برای

[1] Quad-partite integrated whole

[2] Proximity parameters

[3] در دسته بندی بنیادین پارامترهای تهدید، مفهوم نزدیک‌ترین نقطه رویکرد یا همان CPA در حقیقت به مجموعه پارامترهای قصد که در ادامه خواهند آمد تعلق دارند ولی به دلیل برجستگی این پارامترها و اهمیت ویژه‌ای که در کمی

میزان نزدیکی و مجاورت اهداف آشکار شده به دارایی‌ها ارائه می‌دهند. پارامترهای کلاس مجاورت عمدتاً از متغیرهای سینماتیکی استخراج می‌شوند و به همین دلیل همانند آن‌ها دارای عدم قطعیت هستند. پارامترهای کلاس مجاورت همگی حول مفهومی به نام نزدیک‌ترین نقطه رویکرد[1] یا به اختصار **CPA** تعریف می‌شوند [۱۵]. شکل (٤) شیوه تعیین نقطه **CPA** و پارامترهای مجاورتی را نشان می‌دهد.



شکل (٤) : هندسه هدف/دارایی و تعیین فاکتور مجاورتی

CPA نقطه‌ای است که هدف مشخص شده کمترین فاصله خود را با دارایی مشخص شده خواهد داشت به این شرط که جهتگیری فعلی خود را تغییر ندهد. به عبارت دقیق‌تر با مسیری که در حال حاضر برای هدف مورد نظر توسط سامانه‌های رهگیری تخمین زده شده است نقطه **CPA** نزدیک‌ترین نقطه به دارایی خواهد بود اگر مسیر این تخمین برقرار باقی بماند. اگر دارایی مورد نظر را ساکن فرض کنیم نقطه **CPA** نقطه تلاقی فاصله عمودی دارایی تا بردار توسعه یافته سرعت هدف خواهد بود. با تعیین **CPA** مجموعه‌ای از کمیت‌ها بر اساس آن محاسبه می‌شوند که در کمی سازی تهدید بسیار مفید هستند. در ادامه تعاریف و نحوه محاسبه این شاخص‌ها آورده شده است. باید توجه داشت که در انجام این محاسبات فرض شده است که مدل اندازه‌گیری مورد استفاده مدل رنج – سمت است. به عبارت بهتر سنسورهای بکار گرفته شده مقادیر اندازه‌گیری رنج r_{ij} و سمت θ_{ij} را در اختیار می‌گذارند که به ترتیب فاصله و سمت میان هدف **i** و دارایی **j** هستند.

هدف آشکار شده T_i و دارایی A_j را در نظر بگیرید. چنانچه بردار حالت برای این دو به ترتیب به صورت $X_t^{(i)} = [x^i \;\; \upsilon_x^i \;\; y^i \;\; \upsilon_y^i]^T$ برای هدف و $X_a^{(j)} = [x^j \;\; \upsilon_x^j \;\; y^j \;\; \upsilon_y^j]^T$ برای دارایی باشد، بردارهای موقعیت و سرعت زیر برای سهولت در محاسبه کمیت‌های مربوط به تهدید مورد استفاده قرار می‌گیرند:

$$Pos = [Pos_x \;\; Pos_y]^T = [x^i \;\; y^i]^T - [x^j \;\; y^j]^T \quad (۱)$$

$$Vel = [Vel_x \;\; Vel_y]^T = [\upsilon_x^i \;\; \upsilon_y^i]^T - [\upsilon_x^j \;\; \upsilon_y^j]^T \quad (۲)$$

$$Range: r = \sqrt{Pos_x^{\,2} + Pos_y^{\,2}} = \sqrt{(x^i - x^j)^2 + (y^i - y^j)^2} \quad (۳)$$

- زمان مورد نیاز برای اینکه هدف به نقطه **CPA** برسد **Time to CPA – TCPA** نامیده می‌شود:

$$TCPA = \frac{Range\ from\ CPA}{Speed} = \frac{r \times \cos(\theta_{ij})}{\sqrt{Vel_x^{\,2} + Vel_y^{\,2}}} = -\frac{Pos_x \times Vel_x + Pos_y \times Vel_y}{\sqrt{Vel_x^{\,2} + Vel_y^{\,2}}} \quad (٤)$$

- فاصله میان **نقطه فعلی هدف i ام** تا نقطه **CPA** با در نظر گرفتن بردار سرعت ثابت، **Range from CPA** نامیده می‌شود:

$$d^{\,i}_{CPA} = r \times \cos(\theta_{ij}) = \sqrt{(Pos_x + TCPA \times Vel_x)^2 + (Pos_y + TCPA \times Vel_y)^2} \quad (۵)$$

سازی مفهوم تهدید دارند در بسیاری از منابع تحت یک عنوان مجرا مطرح شده و مورد بررسی قرار می‌گیرند.

[1] Closest point of approach - CPA

- زمانی که طول می‌کشد تا هدف پس از ۹۰ درجه چرخش در نقطه **CPA** به دارایی برخورد کند **CPA in unit of time – CPA IUOT** نامیده می‌شود:

$$CPA\ IUOT = \begin{cases} \frac{|\dot{r}_{ij}|}{Speed} & if\ r_{ij} \le 0 \\ 0 & if\ \dot{r}_{ij} > 0 \end{cases} = \frac{r \times \sin(\theta_{ij})}{\sqrt{Vel_x{}^2 + Vel_y{}^2}}$$

$$= \frac{Pos_x \times Vel_y + Pos_y \times Vel_x}{\sqrt{Vel_x{}^2 + Vel_y{}^2}}$$

(۶)

- فاصله تا **CPA** : فاصله میان **نقطه فعلی دارایی** مورد نظر (که در اصطلاح نقطه مطلوب یا نقطه مرجع تهدید نامیده می‌شود) تا نقطه **CPA** یکی از شاخص‌های کلاس مجاورت است که **Range at CPA** نامیده می‌شود.

$$d^{j}_{CPA} = r \times \sin(\theta_{ij})$$
$$= \sqrt{(Pos_x + CPA\ IUOT \times Vel_x)^2 + (Pos_y + CPA\ IUOT \times Vel_y)^2}$$

(۷)

- زمان مانده تا برخورد یا **Time before hit – TBH** زمان مورد نیاز برای هدف برای رساندن خود به نقطه فعلی دارایی است که به صورت حاصل جمع دو زمان معرفی شده **TCPA** و **CPA IUOT** تعریف می‌شود و شاخص بسیار مهمی در کلاس شاخص‌های مجاورتی است:

$$TBH = TCPA + CPA\ IUOT$$

(۸)

- از مهمترین فاکتورهای کلاس قصد پارامترهای سینماتیکی اهداف از جمله تندی[1] است [۲۸, ۴۳]. مجموعه همزمان سرعت و جهتگیری یک هدف، تندی هدف را معرفی می‌کنند. تندی به همراه رنج هدف نسبت به دارایی‌ها می‌تواند معیار بسیار خوبی برای بیان قصد یک هدف باشد. این معیار در اصطلاح قریب الوقوعی یا مشرفیت[2] نامیده می‌شود. اگر r_{ij} رنج میان هدف **i** ام با دارایی **j** ام باشد و $\dot{r}_{ij}$ نرخ تغییرات آن باشد و نیز v_i سرعت هدف **i** ام باشد. معیار مشرفیت با رابطه ۰ تعریف می‌شود [۱۸].

(۹)

- تعداد مانورها یکی دیگر از پارامترهای کلاس قصد برای کمی سازی تهدید است. این پارامتر با توجه به منحنی خط سیری که برای هر هدف توسط سیستم رهگیری به دست می‌آید تعیین می‌شود.
- دسته دیگر از فاکتورهایی که قصد و انگیزه اهداف را ارزیابی می‌کنند، فاکتورهای زمینه‌ای هستند. فاکتورها و معیارهای زمینه‌ای آن‌هایی هستند که در ارتباط با محیط عملیات معنا می‌یابند [۵, ۲۸, ۳۷]. این فاکتورها غالباً به شکل گزاره‌های منطقی طرح شده و مقادیری به شکل صفر یا یک دارند. از جمله این فاکتورها می‌توان به حرکت در مسیر خط هوایی[3] [۲۸]، اقدامات تعاملی اهداف[4] (با سایر اهداف حاضر در صحنه عملیات)، تخلف از مسیر پروازی تعیین شده و سرپیچی از فرامین ترافیک هوایی اشاره کرد.
- روشن بودن و استفاده از رادار کنترل آتش (سلاح) یکی دیگر از پارامترهایی است که می‌تواند حاکی از وجود انگیزه‌های خاص در اهداف باشد. هدفی که با رادار کنترل آتش روشن در صحنه نبرد حضور دارد می‌تواند تهدیدی جدی به شمار رود.
- آمادگی عملیاتی[5] هدف از دیگر پارامترهایی است که می‌تواند در تعیین قصد او در آسیب رساندن به دارایی‌ها حکایت داشته باشد. این پارامترها را می‌توان از انجام اقداماتی توسط اهداف نظیر: سوخت گیری هوایی و خاموش کردن ارتباطات رادیویی استنباط کرد.
- ردپای خیس یا خشک[6] که به معنای عبور اهداف از روی خشکی و یا سطح آب است نیز می‌تواند در تعیین قصد

[1] Velocity
[2] Imminence
[3] Following air lane or corridor
[4] Coordinated activities
[5] Operational readiness
[6] Feet wet/dry

اهداف مورد استفاده قرار گیرد. این پارامتر کمک می کند تا مبدأ حمله یا هدف حمله کننده مشخص شود. همچنین تعیین ردپای خیس یا خشک علاوه بر تعیین محل شروع اقدام به تعیین استعداد و نوع پشتیبانی از هدف مورد نظر نیز اشاره دارد.

- حمل یا همراه داشتن سلاح که در اصطلاح نظامی بال آلوده یا پاک[1] نامیده می‌شود، فاکتور مهمی در ارزیابی نیت و قصد بازیگران در صحنه نبرد است. بازیگران می‌توان به مقاصدی چون شناسایی، تخریب و یا فریب وارد صحنه عملیات شوند که برای انجام همه آن‌ها نیازی به مسلح بودن نیست.
- استفاده از روش‌ها و تکنیک‌های فریبکارانه یا عملیات ایذایی توسط اهداف می‌تواند عامل دیگری در تبیین قصد اهداف در کمی سازی تهدید باشد. از جمله این عملیات می‌توان حرکت درست روی خط مرزی را نام برد.
- رهاسازی پارازیت یا جمینگ برای مختل کردن عملکرد رادارها از دیگر فاکتورهایی است که می‌تواند در ارزیابی قصد اهداف در صحنه نبرد مورد استفاده قرار بگیرد. همچنین کلیه تاکتیک‌ها و تکنیک‌هایی که برای پنهان ماندن یا فریب دادن سنسورهای مورد استفاده در سامانه‌های رهگیری بکار برده می‌شود، می‌تواند شاخص‌های مناسبی برای ارزیابی قصد اهداف در صحنه عملیات باشد.
- فاصله هدف از سایر واحدهای پشتیبانی دشمن نیز می‌تواند در ارزیابی قصد هدف به کار گرفته شود. به این معنا که هرچه هدف از واحدهای پشتیبانی خودی‌اش دورتر باشد یعنی ریسک بیشتری را برای خود خریده و در نتیجه احتمال وجود تهدید از جانب چنین هدفی برای دارایی‌ها وجود دارد.
- آرایش اهداف در ارتباط با هم نظیر حرکت اسکادرانی از جنگنده‌ها یا ناوگروه‌ها نیز باید از ابتدای حرکت آن‌ها از مبدأ تحت پایش و آنالیز باشد. وجود قصد تهاجم و حمله به مایملک و دارایی‌ها را می‌توان از شکل آرایش جنگی و میزان و نحوه فضاسازی آن‌ها استنباط کرد.
- کشور و مبدأ حرکت اهداف می‌تواند اطلاعات مهمی از قصد و انگیزه آن‌ها به همراه داشته باشد. اهداف متعلق به کشورهای مبدأیی که در فضای دیپلماتیک با آن‌ها تنش وجود دارد، می‌تواند نامزد تخصیص میزان تهدید بالایی باشند.
- با شناسایی کشور مبدأ اهدافی که در صحنه نبرد و عملیات حضور دارند می‌توان از اطلاعات قبلی در این زمینه بهره برد و فاکتور دیگری در تعیین قصد معرفی کرد. در صورتی که پیش‌تر از صحنه فعلی، تهاجمی توسط نیروهای خودی متوجه مایملک و دارایی‌های کشور مبدأ اهداف شناسایی‌شده، شده باشد، در این صورت میزان تهدید تخصیص یافته به این اهداف بسیار بیشتر خواهد بود.
- شناسه دوست/دشمن[2] یکی دیگر از پارامترهایی است که به شکل مستقیم از سامانه‌ای با همین عنوان از هدف دریافت می‌شود. این سامانه منطبق بر یک سیستم رمزنگاری شده اقدام به پرسش از اهداف کرده و اهداف نیز بر اساس پروتکل رمزنگاری مناسب، پاسخی تولید و ارسال می‌کنند. تعیین شناسه دوست/دشمن پس از آنالیز پاسخ دریافتی از هدف انجام می‌گیرد.
- موارد بسیاری دیگری را نیز می‌توان در تعیین قصد اهداف برشمرد. در منابع مواردی نظیر حرکت هدف موازی با رادار، ارسال کدهای فریب دهنده مبنی بر شناسه دوستی در سیستم **IFF** و تمایل اهداف برای حرکت در ارتفاعی پایین‌تر از ارتفاع قابل تشخیص برای رادار می‌تواند برای ارزیابی قصد اهداف و در نتیجه در تبیین میزان تهدید آن‌ها مورد استفاده قرار بگیرد [۳۷, ٤۳].

۳-٤-۲. شواهد ارزیاب توانمندی

مجموعه دیگری از پارامترها برای کمی سازی تهدید پارامترهای کلاس توانمندی یا قابلیت هستند. این کلاس از پارامترها به توانایی اهداف برای تهدید و وارد آوردن آسیب به دارایی‌ها باز می‌گردند [۱۰, ۱۱, ۱۸]. پارامترهای توانمندی در حقیقت به دنبال پاسخ برای این سؤال هستند که اهداف دشمن

[1] Wings clean/dirty

[2] Identification Friend or Foe – IFF

یا نیروهای متخاصم از چه تکنولوژی‌هایی برخوردار هستند، از چه تاکتیک‌هایی استفاده می‌کنند و چه تکنیک‌هایی به کار می‌برند. پیش‌بینی تکنولوژی، تکنیک و تاکتیک اهداف[1]، تبیین کننده بخش مربوط به توانمندی تهدید هستند. این پارامترها در پی دستیابی به اطلاعاتی پیرامون اینکه قابلیت بکارگیری و تأثیر گذاری آنچه در دست طرف مقابل است (اعم از تکنولوژی، تکنیک‌های نبرد و تاکتیک‌های عملیاتی) چه میزان خواهد بود.

- پارامتر مرکزی در این کلاس شناسایی نوع هدف است. شناسایی نوع و ماهیت اهداف می‌تواند با در اختیار داشتن اطلاعاتی نظیر شناسایی دوست/دشمن[2]، داده‌های **ESM** و یا ویژگی‌های خاص سینماتیکی نظیر شتاب و نوع مانورها تعیین شود.
- پس از اینکه ماهیت و نوع هدف تعیین شد نوبت به تعیین استعداد تسلیحاتی هدف می‌رسد که در حقیقت می‌بایست نوع و برد عملیاتی سلاح‌های هدف[3] به درستی تعیین شود. اهدافی که برد و پوشش سلاح‌های آن‌ها به گونه‌ای است که می‌توانند دارایی‌های خاصی مورد تهاجم قرار دهند نسبت به اهدافی که هیچ دارایی حفاظت شده‌ای در تیررس آن‌ها نیست، از میزان تهدید بالاتری برخوردار هستند. تسلیحات هدف از جمله مهم‌ترین پارامترها در تعیین میزان توانمندی او بشمار می‌رود. در این میان هندسه پوش تسلیحاتی اهداف[4] نسبت به دارایی که قرار است مورد حفاظت قرار گیرند بسیار مهم است. نوع تسلیحات (میزان کشندگی) یکی دیگر از مواردی است که مورد ارزیابی قرار می‌گیرد.
- میزان/ظرفیت حمل مهمات یا در اصطلاح نظامی میزان شارژ انفجاری[5] یکی دیگر از پارامترهای مهم در تعیین قابلیت کشندگی اهداف در صحنه عملیات است.
- حداکثر برد (پوش) سلاح[6]های در اختیار هدف یکی از فاکتورهایی است که همراه با شاخص‌های فاصله و سرعت می‌تواند در آنالیز میزان توانمندی اهداف در ایجاد تهدید برای مایملک و دارایی خودی بکار رود.
- میزان تحرک‌پذیری[7] به معنایی اینکه که هدف در صحنه عملیات از چه گستره جغرافیایی امنی برخوردار است و چه میزان می‌تواند در این گستره جابجایی داشته باشد از دیگر پارامترهای تعیین کننده توانمندی اهداف است. چالاکی و ظرفیت مانور[8] هدف که وابسته به نوع هدف است از دیگر مواردی است که در ارزیابی میزان توانمندی مورد استفاده قرار می‌گیرد. به عنوان مثال اهداف هوایی، زمینی، شناور و زیرسطحی به ترتیب از قدرت و ظرفیت مانورپذیری بیشتری برخوردار هستند.
- گستره دید در میدان عملیات[9] نیز از فاکتورهای تعیین کننده در میزان توانمندی اهداف به شمار می‌رود. این معیار به معنای میزان تسلط و آگاهی اهداف از صحنه عملیات است و همانطور که پیش‌تر ذکر شده به تکنولوژی ها، تاکتیک‌ها و تکنیک‌هایی که اهداف برای کسب اطلاعات از محیط عملیات بکار می‌برند، وابسته است.
- پوشش زرهی[10] اهداف در برابر تسلیحات طرف مقابل معیار دیگری است که برای سنجش توانمندی اهداف مورد استفاده قرار می‌گیرد.
- ظرفیت سوخت[11] اهداف یکی دیگر از پارامترهای کلاس توانمندی به شمار می‌رود که البته در تعیین نوع اهداف نیز بسیار کاربرد دارد. میزان ظرفیت سوخت یک هدف در

[1] Technology, technique and tactic (T3) forecasting

[2] شناسایی دوست/دشمن (Identification Friend or foe - IFF) یک سیستم امن برای شناسایی اهداف هوایی است. این سیستم با استفاده از تجهیزات الکترومغناطیسی و فرکانس رادیویی RF با اهداف هوایی ارتباط برقرار می‌کند. این سیستم در حقیقت یک سیستم شناسایی مبتنی بر رمز است که با ارسال سیگنال به اهداف هوایی (Chalenging signal) منتظر دریافت پاسخ یا رمز صحیح می‌ماند.

[3] Weapon type and weapon envelope

[4] Target weapon envelope geometry

[5] Amount of explosive charge

[6] Weapon envelop

[7] Mobility

[8] Agility and maneuver capacity

[9] Field of view

[10] Armor type

[11] Fuel capacity

تعیین محدوده و حداکثر شعاعی[1] که آن هدف می‌تواند به اجرای عملیات بپردازد استفاده می‌شود.

برای محاسبه امتیاز یک هدف در میزان توانمندی منابع زیادی در دسترس نیست. کمی کردن پارامترهایی که اشاره شد می‌تواند در پژوهش‌های آتی با جزئیات بیشتری مورد توجه قرار بگیرد. در [٤٧] تابعی برای ارزیابی میزان توانمندی یک هدف بر اساس میزان وجوه مختلف توانمندی وزن دهی آن‌ها بر اساس احتمال بکارگیری آن‌ها در شرایط محیط عملیاتی ارائه شده است. در [١٨] توابع بسیار ساده‌ای برای ارزیابی میزان قابلیت و قصد اهداف مورد اشاره قرار گرفته است. این توابع بر حسب متغیرهای سینماتیکی هدف نظیر سرعت و رنج شکل یافته‌اند.

٣-٤-٣. فاکتورهای تحمل‌پذیری

یک بازیگر (یا گرداننده آن) در صحنه عملیات چنانچه قصدی برای انجام یک اقدام تهدید آمیز داشته باشد، لازم است تا ابتدا به محاسبه سود و زیان آن بپردازد. به عبارت دقیق‌تر هنگامی که یک بازیگر قصد و انگیزه‌ای برای ایجاد تغییر در شرایط صحنه عملیات را دارد پیش آن که اراده او بر این تعلق بگیرد که اقدامی را در راستای ایجاد این تغییرات انجام دهد می‌بایست سود و زیان این اقدامات و شرایط ایجاد شده را ارزیابی کند. محاسبه هزینه یک بازیگر در انجام مجموعه‌ای از اقدامات خاص که برای دستیابی به اهداف خاصی صورت می‌گیرد ارتباط بسیار نزدیکی با عامل‌های دیگر تهدید نظیر قصد و فرصت دارد. اقدام یک بازیگر در صحنه عملیات همانطور که پیش‌تر گفته شد موجب تغییر در شرایط محیط عملیاتی و همچنین واکنش سایر بازیگران خواهد شد. حال پرسش اینجاست که آیا اقدام سایر بازیگران در تقابل با این بازیگر از یک سو و تغییراتی که در نتیجه برآیند اقدامات انجام شده از سوی بازیگر ابتدایی و سپس سایر بازیگران در محیط عملیاتی حادث خواهد شد، برای بازیگر نخست ارزش آفرینی قابل توجهی خواهد داشت یا خیر؟ از این رو برای ارزیابی دقیق‌تر این که حضور یک موجودیت یا وقوع یک رخداد در صحنه عملیات و اقدامات و تأثیراتی که پیامد این حضور است چه هزینه‌هایی برای سایر بازیگران و خود آن موجودیت خواهد داشت و همچنین اینکه این مجموعه تأثیرات برای کدامین موجودیت‌ها قابل پذیرش و تحمل خواهد بود فاکتورهای کلاس تحمل‌پذیری پدید می‌آیند. باید اشاره کرد که مجموعه این آنالیزها با نگاه به این که موجودیتی که در پی محاسبه تهدید برای اقدامات او هستیم چه سطحی از سه عنصر تکنولوژی، تکنیک و تاکتیک را در اختیار دارد، انجام می‌پذیرد. در آنالیز تحمل‌پذیری نهایتاً همه چیز به شکل هزینه در نظر گرفته می‌شود. در نظر گرفتن فاکتورهای تحمل‌پذیری به شکل هزینه کمک می‌کند تا مشخص شود آیا هزینه یک تهدید برای محاسبه‌گر قابل تحمل هست یا خیر؟ و نیز اینکه آیا مقابله با تهدید و خنثی‌سازی آن و اقداماتی که در تقابل با آن تهدید می‌توان انجام داد برای محاسبه‌گر دارای هزینه‌های قابل تحملی خواهد بود یا خیر؟

در ادامه به ارائه شاخص‌های پیشنهادی برای تحلیل تحمل‌پذیری خواهیم پرداخت.

- **هزینه اقدام**: هزینه‌ای (تخمینی) که انجام اقدام پیش‌بینی شده برای خود بازیگر هدف دارد (نظیر هزینه بکارگیری تسلیحات، هزینه ناشی از آسیب به بازیگر یا از بین رفتن خود او، هزینه‌ای که متوجه واحدهای پشتیبان بازیگر و واحدهای همسو با او خواهد شد) یا اختصاراً *هزینه کنش*[2]. هزینه کنش می‌تواند در چهار دسته هزینه‌های فیزیکی، هزینه‌های اجتماعی، هزینه‌های اقتصادی و هزینه‌های زیست محیطی لحاظ شود.
- **منفعت اقدام**: میزان آسیب و خسارت ناشی از اقدام پیش‌بینی شده یک بازیگر برای دارایی‌ها تحت حفاظت خودی یا میزان آورده استراتژیک برای بازیگر منشأ در محیط عملیاتی (نظیر برتری موقعیت، تصرف سرزمین یا دارایی، حذف اشخاص کلیدی).
- **هزینه دفاع**: هزینه انجام اقدامات متقابل برای جبران یا خنثی سازی اقدام پیش‌بینی شده از سوی بازیگر هدف برای خودی یا اختصاراً *هزینه واکنش*[3].

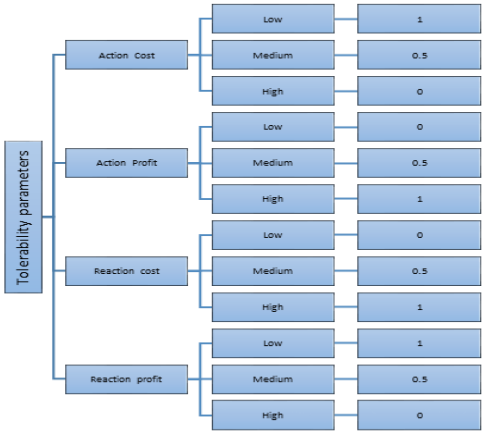
[1] Maximum radius of operation

[2] Action cost

[3] Reaction cost

- **منفعت دفاع**: میزان سود ناشی از اقدام و یا میزان خسارتی که در صورت اجرای اقدام متقابل از آن پیشگیری و ممانعت به عمل می‌آید.

تصویر شکل (۵) نمودار درختی اختصاص مقادیر گسسته به پارامتر تحمل‌پذیری را نشان می‌دهد.



شکل (۵) : شاخص‌های ارزیاب تحمل‌پذیری

۳-٤-٤. فاکتورهای فرصت

در ارزیابی فرصت، هدف این است که فضای عملیاتی را از حیث وجود شرایط و امکان به کار بستن تکنولوژی‌ها، تکنیک‌ها و تاکیک‌های مورد نظر بررسی کنیم [۸]. به عبارت بهتر فرصت سنجی بستری برای آزمودن مقاصد و انگیزه‌ها از یک سو و توانمندی و قابلیت بازیگران حاضر در صحنه از سوی دیگر است. بنابراین فرصت سنجی، مجموعه فعالیت‌های هدفمندی نظیر: کسب اطلاعات از برنامه دشمن، تحلیل و پیش دستی در به دست آوردن موقعیت‌های فضایی و مکانی مطلوب، تحلیل جایگیری و آرایش نیروهای دشمن و ارزیابی ظرفیت‌های رفتاری[1] بازیگران صحنه عملیات خواهد بود. برای ارزیابی فرصت مجموعه از تحلیل‌های فضایی-زمانی انجام می‌شود تا مشخص گردد که آیا پیوستگی و تجمیع موقعیت‌ها و شرایط مطلوب برای بازیگران صحنه عملیات به نوعی هست که بتوانند اهداف و نیت‌های خود را عملی کنند. از جمله این تحلیل‌ها می‌توان به آنالیزهای محیطی اشاره کرد. در تحلیل‌های محیطی اثر عواملی مانند شرایط آب و هوایی، شرایط جغرافیایی و عوارض زمین بر امکان انجام مأموریت و تحقق اهداف آن پرداخته می‌شود. این که این عوامل چه تأثیری بر دامنه و وسعت دید، دقت اندازه‌گیری سنسور ها، میزان تحرک بازیگران حاضر در صحنه و نهایتاً عملکرد تسلیحات دارند برای تحقق یک فرصت باید به طور کامل ارزیابی شوند. در [٤٧] اشاره شده است که شرایطی که تعیین کننده وجود یا عدم وجود فرصت برای عملیاتی کردن قصدها هستند به صورتی سطوحی از آمادگی تکنولوژیک[2] بیان می‌شوند. این سطوح آمادگی به نه دسته تقسیم شده و بر مبنای آن یک تابع امتیاز به مفهوم فرصت تخصیص داده شده است.

از دیگر فاکتورهایی که برای ارزیابی فرصت مورد استفاده قرار گرفته می‌توان به امکان انجام (هم از حیث زمانی و هم از حیث فضایی) مانور لازم برای بکارگیری یک سلاح خاص [۱۵]، در اختیار داشتن اطلاعاتی از برنامه سایر بازیگران حاضر در صحنه، زمانبندی موقعیت‌ها و اقدامات[3] و خط دید[4] [۹, ۱٦] اشاره کرد. همچنین گزارشاتی که از سازمان‌های اطلاعاتی دریافت می‌شود می‌تواند به تحلیل‌های زمان/فضایی کمک کند [٤].

۳-٤-۵. جمع بندی فاکتورهای کلاس مختلف در ارزیابی تهدید و ارکان آن

در بخش‌های پیشین به مواردی از پارامترهای مختلف برای ارزیابی ارکان تهدید یعنی قصد، توانمندی، تحمل‌پذیری و فرصت اشاره شد.

فاکتورهای مؤثر در ارزیابی ارکان تهدید محدود به این موارد نخواهد بود اما طرح بخش زیادی از این پارامترها در کنار هم می‌تواند در ایجاد یک بینش استدلالی مناسب پیرامون ماهیت تهدید و نحوه ارزیابی آن بسیار مؤثر باشد [٤]. همانطور که اشاره شد، بسیاری از این پارامترها کیفی هستند و تعیین معیار و شاخصی کمّی برای آن‌ها به راحتی ممکن نیست. تنها برای عده‌ای محدود از آن‌ها (نظیر **CPA**) توابع امتیاز دهی و شاخص‌های شناخته شده کمّی وجود دارد. به همین دلیل است که عمده ارزیابی‌ها و تحلیل‌های پیرامون تهدید توسط اپراتورهای خبره صورت می‌پذیرد. نگاه به عمده پژوهش‌ها در

[1] Behavioral capacity

[2] Technology readiness level – TRL

[3] Spatiotemporal states of situation

[4] Line of sight

حوزه ارزیابی تهدید نشان می‌دهد که **CPA** به عنوان کلیدی‌ترین عنصر در ارزیابی و تحلیل تهدید مورد استفاده قرار می‌گیرد. اما بسیاری دیگر از شاخص‌های کلیدی دیگر در **CPA** و پارامترهای وابسته به آن منعکس نشده‌اند. تحلیلی از تهدید که تنها بر اساس فاکتورهای مجاورتی استوار باشد، به نتایج دقیقی منجر نمی‌شود و موجودیت‌هایی که دارای فاکتورهای مجاورتی یکسانی هستند دارای تهدید مشابهی ارزیابی می‌شوند در حالی که ممکن است به طرز قابل توجهی متفاوت باشند. این نکته در بکارگیری پهپاد های رزمی به وضوح قابل مشاهده است. پهپاد هایی که دقیقاً با الگوهای رفتاری یک مهاجم واقعی در صحنه عملیات طراحی می‌شوند ولی ارزش بسیار پایینی دارند و صرفاً جهت مقاصدی چون فریب، انباشت اطلاعات بلااستفاده، اشغال ظرفیت‌های محاسباتی و تحلیلی، سرریز شدن ظرفیت سیستم‌ها و سنسورها و نهایتاً هدرفت پتانسیل‌های تسلیحاتی بکار می‌روند. لذا طراحی گزاره‌های منطقی بر اساس سایر فاکتورها و معیارهای تشکیل دهنده تهدید و ارزش‌گذاری آن‌ها به صورت شواهدی با چند مقدار محدود گسسته می‌تواند در انعکاس کلیه این فاکتورها در ارزیابی تهدید بسیار مؤثر عمل کند. این گزاره‌های منطقی ضمن اینکه به واقعی‌تر شدن ارزیابی تهدید کمک می‌کنند، به دلیل ساده‌گی ارزش گذاری‌شان بار ادراکی محسوسی را برای اپراتور ایجاد نخواهند کرد.

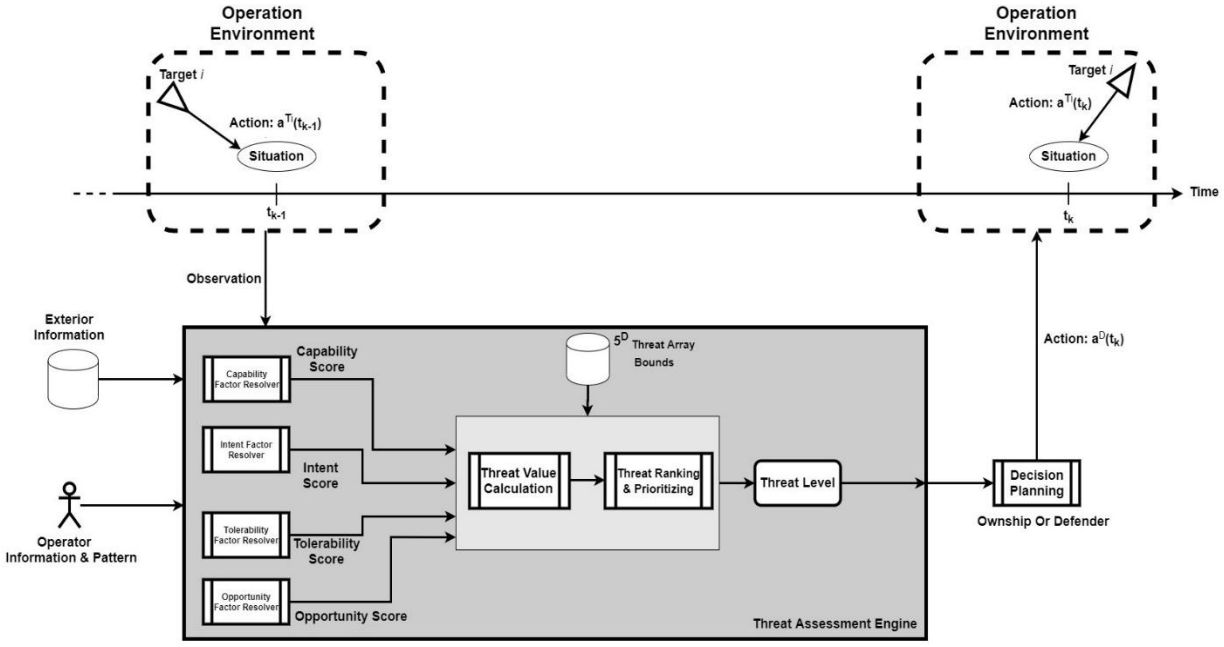
در جدول (۱) جمع‌بندی فاکتورهای مؤثر در ارزیابی ارکان تهدید گردآوری شده است.

جدول (۱) : جمع‌بندی فاکتورهای مؤثر در ارزیابی ارکان تهدید

ردیف	کلاس فاکتور	عنوان پارامتر		عنوان لاتین
۱	پارامترهای کلاس قصد (Intent parameters)	پارامترهای مجاورتی (Proximity parameters)	نزدیک‌ترین نقطه رویکرد	Closest point of approach - CPA
			فاصله هدف تا نقطه رویکرد	Range from CPA – d^{i}_{CPA}
			فاصله دارایی تا نقطه رویکرد	Range at CPA - d^{j}_{CPA}
			فاصله زمانی هدف تا نقطه رویکرد	Time to CPA – TCP
			فاصله زمانی هدف از نقطه رویکرد تا دارایی	CPA in unit of Time – CPA IUOT
			زمان تا وقوع برخورد هدف و دارایی	Time before hit – TBH
		سرعت، جهتگیری و رنج (مشرفیت)		Speed, heading and range - imminence
		تعداد مانور ها		Number maneuvers
		حرکت در مسیر خط هوایی		Following air lane or corridor
		تخلف از مسیر پروازی تعیین شده		deviation of specified/designated flight path
		سرپیچی از فرامین رادیویی ترافیک		Violation of radio traffic command
		اقدامات تعاملی با سایر اهداف		Coordinated activities
		ردپای خیس/خشک		Wet feet / Dry feet
		حمل سلاح		Wings Clean/dirty
		استفاده از رادار کنترل آتش		Detection of fire control radar (FCR) emission
		آمادگی عملیاتی(سوختگیری هوایی)		Arial refueling
		رهاسازی پارازیت/جمینگ		Jamming
		عملیات فریبکارانه		Use of deception/ spoofing
		حرکت در ارتفاع بسیار پایین		Very low altitude
		حرکت موازی با رادار شناسایی		Fly tangential to the radar
		پدیداری (قابلیت مشاهده و دیدن)		Visibility
		فاصله هدف تا واحدهای پشتیبانی دشمن		Own support
		آرایش اهداف		Deployment
		پاسخ به اقدام تهاجمی قبلی		Retaliate/Invasion response
		رمزنگاری دوست/دشمن		Identification friend or foe - IFF
		کشور و مبدأ حرکت هدف		Origin location
۲	پارامترهای کلاس توانمندی (Capability parameters)	نوع هدف		Target type
		نوع (استعداد) تسلیحات		Target weapon lethality
		میزان شارژ انفجاری		Amount of explosive charge
		پوش (برد) تسلیحات		Target weapon envelope
		تحرک پذیری، چالاکی و قدرت مانور		Mobility/ Maneuverability
		گسترده دید عملیاتی		Field of view - FOV
		پوشش زرهی		Armor type
		ظرفیت سوخت		Fuel capacity
۳	فاکتورهای تحمل‌پذیری (Tolerability parameters)	هزینه اقدام		Action cost
		منفعت اقدام		Action profit
		هزینه دفاع یا اقدام متقابل		Reaction cost
		منفعت دفاع یا اقدام متقابل		Reaction profit
٤	پارامترهای کلاس فرصت (Opportunity parameters)	شرایط آب و هوایی		Weather/climate condition
		شرایط جغرافیایی و عوارض زمین		Geographical and terrain condition
		زمانبندی موقعیت ها		Situation timing
		امکان انجام مانور خاص		Special maneuver possibility
		اطلاع از برنامه اقدامات بازیگران در صحنه		Knowledge of enemy's plans
		فضای سیاسی و دیپلماتیک		Political condition
		گزارش سازمان‌های اطلاعاتی		Intelligence reports

۳-۵. موتور ارزیاب منطقی مبتنی شواهد گسسته مقدار

در بخش‌های گذشته بحث تفضیلی پیرامون ارکان تهدید و فاکتورهای آن انجام شد. تهیه لیست جامعی از فاکتورهای مؤثر بر تهدید بخش بسیار مهم و حیاتی از فرآیندی است که برای کمی سازی تهدید دنبال می‌شود. مجموعه فاکتورهایی که محتوای لیست اشاره شده را تشکیل می‌دهند برای اینکه اثر خود را در ارزیابی تهدید منعکس کنند به صورت سوال‌هایی با پاسخ گسسته تغییر قالب داده‌اند. این سؤال‌ها به صورتی طراحی شده‌اند که دارای پاسخی به شکل صفر (خیر)، نیم (میانه) یا یک (بله) باشند. سپس این سؤالات توسط موتور منطقی ارزیابی شده و منجر به تولید یک خروجی برای هر یک از ارکان تهدید خواهد شد. همچنین سؤالات می‌توانند به صورت ترکیب وزنی مشخصی مورد ارزیابی قرار بگیرند. به این معنا که پاسخ به هر سؤال دارای تأثیر مشخصی در خروجی نهایی ارزیابی آن رکن از تهدید داشته باشد. وزن دهی این امکان را فراهم می‌آورد تا فاکتورهای مهم‌تر نقش برجسته‌تری در شکل‌گیری تهدید نهایی داشته باشند. پس از ارزیابی ارکان تهدید توسط موتور منطقی با استفاده از نظرات نخبگان و متخصصان این حوزه بازه‌هایی برای هر کدام از ارکان تهدید در نظر گرفته شده و میزان تهدید نهایی ناشی از مقدار ارزیابی شده برای هر رکن به صورت یک ماتریس سه بعدی محاسبه می‌شود. نمودار بلوکی این فرآیند در شکل (٦) آمده است. این نمودار بلوکی ساختار و معماری سیستم ارزیابی تهدید در این پژوهش را به تصویر می‌کشد. زمان در صحنه عملیات توسط نوار زمانی **Time** نشان داده شده است. در لحظه t_{k-1} صحنه عملیات با اقدامی ($a^{T_i}(t_{k-1})$) که توسط یکی از اهداف (**Target** i) انجام می‌دهد دستخوش تغییر شده و موقعیت تاکتیکی جدیدی خلق می‌شود. این شواهد توسط ارزیابی‌کننده تهدید که همان خودی است به طور پیوسته مشاهده می‌شود. شواهد مشاهده‌شده دسته‌بندی شده و به صورت ورودی در اختیار توابع مربوطه قرار می‌گیرد. هر ماژول با استفاده از شواهد اختصاصی خود به تحلیل رکن متناظر تهدید خود می‌پردازد و سپس مجموعه امتیازات نهایی حاصل برای ارزیابی و اولویت‌بندی تهدید در اختیار تابع ارزیاب تهدید قرار می‌گیرد. تحلیل‌ها و محاسبات صورت گرفته در سیستم ارزیاب تهدید منجر به تولید یک لیست اولویت‌بندی شده از تهدیدات خواهد شد که در اختیار تصمیم‌گیران قرار می‌گیرد تا برنامه عملیاتی متناسب با آن ایجاد شود. اقدام متقابل ($a^{D}(t_k)$) در راستای برنامه عملیاتی صادر و اجرا می‌شود. این اقدام در لحظه زمانی t_k اثر خواهد گذاشت و صحنه عملیات را تغییر داده و موقعیت تاکتیکی جدیدی را به وجود می‌آورد. این فرآیند در طول زمان عملیات به شکل پیوسته تداوم می‌یابد.



شکل (٦) : نمودار بلوکی فرآیند ارزیابی و تخمین تهدید

موتور منطقی اشاره شده برای اینکه بتواند میزان تهدید را از فاکتورهای تشکیل دهنده آن ارزیابی کند لازم است تا ورودی‌هایی به شکل گزاره‌های صفر یا یک داشته باشد. این ورودی‌ها همان فاکتورهای تهدیدی هستند. موتور ارزیاب منطقی از فاکتورهای تهدید به عنوان ورودی خود استفاده می‌کند. فاکتورهای تهدید که تعیین کننده ارکان تهدید یعنی توانمندی، قصد، تحمل‌پذیری و فرصت هستند باید به شکل گزاره‌هایی منطقی تغییر ساختار یابند تا بتواند برای موتور ارزیاب قابل فهم باشند. در شکل (٥) نمونه ای از تخصیص مقادیر گسسته به گزاره‌هایی منطقی برای هرکدام از فاکتورهای ارزیاب رکن تحمل‌پذیری اشاره شده در جدول (١) طراحی شده است. گزاره‌های منطقی طراحی شده برای اینکه بتوانند توسط ماشین استنتاج منطقی قابل استفاده باشند باید در ساده‌ترین حالت ممکن باشند. این بدان مفهوم است که تفسیر این گزاره‌ها باید به راحتی صورت بگیرد و هیچ گونه ابهامی در پاسخ به آن‌ها وجود نداشته باشد. از این رو پیش از طراحی این سؤالات باید موارد زیر را در نظر داشت:

- برای تفسیر برخی از فاکتور ممکن است نیاز به ساختار سلسله مراتبی باشد. به عبارت دیگر برای وجود امکان پاسخ به یک گزاره (متناظر با یکی از فاکتورهای تهدید) لازم است تا گزاره‌هایی ماقبل از آن تفسیر شده باشند.
- ممکن است زنجیره‌ای از گزاره‌ها برای تفسیر یک فاکتور نیاز باشد.
- فاکتورهایی که نیاز به مقدار دهی دارند توسط داده‌های در دسترس و نیز تجربیات اپراتور مقدار دهی می‌شوند.

پس از اینکه تمامی فاکتورهای اشاره شده برای یک هدف خاص ارزیابی شد سپس مجموعه پارامترهای هر رکن از تهدید برای تولید یک شاخص امتیاز با هم دیگر جمع شده و سپس با توجه به تعداد پارامترهای آن رکن نرمالیزه می‌شوند. در نهایت پنج شاخص امتیاز به ازای هر رکن تهدید تولید می‌شود که هر کدام مقداری در بازه [0 1] خواهند داشت. این شاخص امتیاز طبق رابطه ١٠ با استفاده از مقادیر اختصاص یافته به هر فاکتور محاسبه می‌شود.

$$Score_X = \frac{1}{N}\sum_{i}^{N} W_x^{\,i} \times TF_x^{i} \qquad (١٠)$$

که در آن **x** رکن تهدید، **N** تعداد کل فاکتورهای تهدید برای هر رکن، $\mathbf{TF^i_x}$ مقدار اختصاص یافته به هر فاکتور تهدید و $\mathbf{W^i_x}$ وزن اختصاص یافته به هر فاکتور تهدید بنا به نظر اپراتور است. وزن‌ها مقادیری بین صفر و یک دارند و برای افزایش تأثیر یک فاکتور در امتیاز نهایی رکن تهدید مورد نظر بکارگرفته می‌شوند. پس از محاسبه مقدار هر رکنی از تهدید، یک آرایه ٥ بعدی از بازه‌های تعیین شده توسط اپراتور برای تعیین میزان تهدید اختصاصی هر هدف بکار گرفته می‌شود. این آرایه از سه بازه برای هرکدام از ارکان تهدید تشکیل یافته است که در مجموع ٢٤٣ مقدار خواهد داشت. پس از تعیین میزان تهدید برای هر هدف، لیستی از اهداف و تهدیدهای متناظر با آن‌ها خواهیم داشت که به راحتی می‌توان بر اساس میزان تهدید آن‌ها را اولویت‌بندی کرد. لیست اولیه اهداف در انتها به یک لیست اولویت‌بندی شده بر اساس تهدید تبدیل می‌شود.

٤. شبیه سازی یک سناریو تهدیدی

در ادامه برای ارزیابی روش ارائه شده و سنجش میزان کارایی موتور منطقی پیشنهادی یک سناریوی فرضی که در بردارنده انواع مختلفی از اهداف تهدیدی باشد را در نظر می‌گیریم. محیط عملیاتی در این سناریو یک صحنه نبرد دریایی است که در آن تنها یک شناور خودی در معرض اهداف تهدیدی متنوعی قرار دارد. شناور از نوع ناوچه[1] جنگی است که در محیط دریایی دور از نواحی ساحلی قرار دارد. اهداف مختلف با مأموریت‌های مختلفی در صحنه نبرد حضور دارند. چنین صحنه‌ای در شکل (٧) به تصویر کشیده شده است. در این سناریو دوازده هدف با ویژگی‌های مختلف در نظر گرفته شده‌اند. همه این اهداف به یک مبدأ تعلق دارند و همه آن‌ها به

[1] Frigate

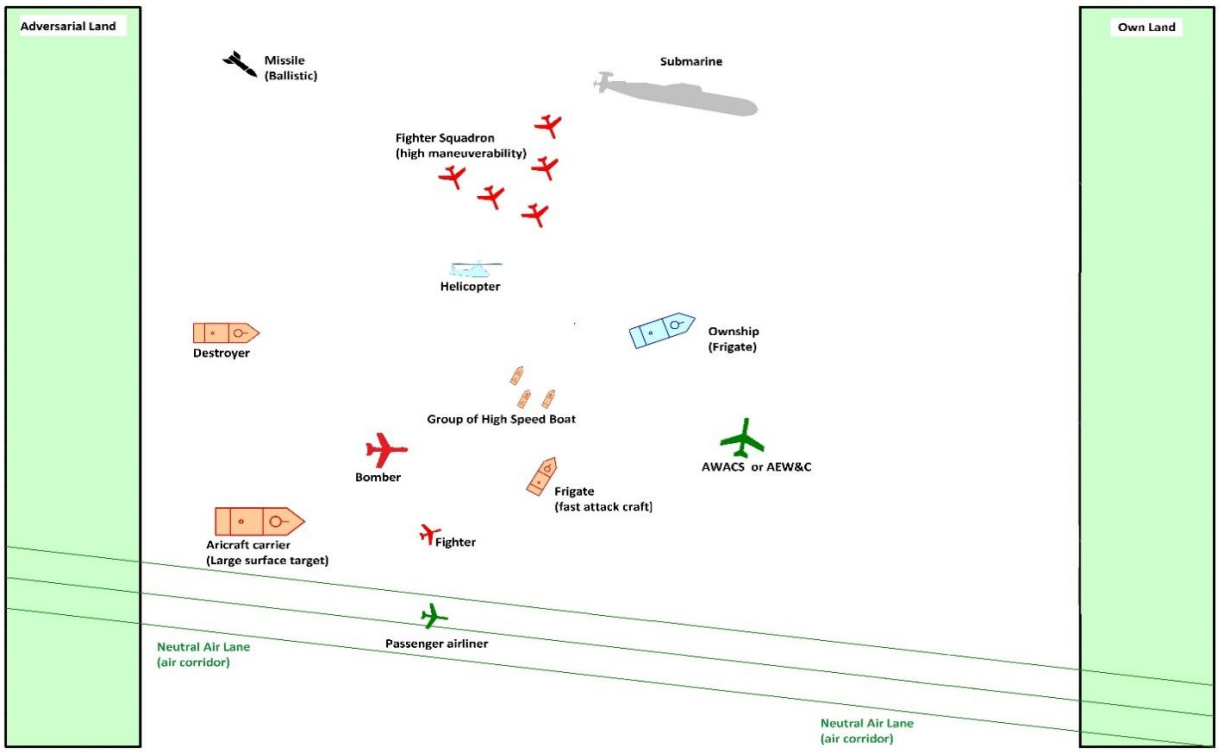
فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال XX ، شمارهٔ XX فصل XXXX

طور پیش فرض تهدیدی در نظر گرفته شده‌اند. هدف از این سناریو ارزیابی تهدید برای هرکدام از این اهداف است. طبق مدل و ساختار معرفی شده در شکل (٦) مشاهدات در یک لحظه از زمان در نظر گرفته می‌شوند و شواهدی که مبنای ارزیابی ارکان تهدید قرار می‌گیرند در همین لحظه شکل می‌یابند سپس این فرآیند برای ارزیابی تهدید در لحظات دیگر تکرار می‌شود. بیش از چهل فاکتور در قالب شواهد ارزیابِ تهدید در نظر گرفته شده و امتیاز دهی شده‌اند. در انتخاب و چینش اهداف در صحنه عملیات سعی شده است تا کلیه شواهد به نوعی مورد استفاده قرار گرفته و نقش داشته باشند.

برای ارزیابی میزان تهدید متناظر با هر هدف لازم است فرضیات زیر را در نظر گرفته شده است:

- فرض ١: تمامی اهداف مشخص شده توسط سامانه‌های مرتبط کشف، آشکارسازی و رهگیری شده‌اند (تعداد اهداف مشخص شده است).
- فرض ٢: نوع اهداف توسط اطلاعات در دسترس و اپراتورها مشخص شده است.
- فرض ٣: تمامی اهداف مشخص شده به یک مبدأ و سرزمین تعلق دارند.
- فرض ٤: شناور خودی در صحنه عملیات تنها بر توان و ظرفیت‌های خود متکی است و فاقد عوامل پشتیبانی است.
- فرض ٥: کل فضای عملیاتی مورد نظر از دید شناور خودی مشاهده پذیر است.
- فرض ٦: تمامی اهداف مقاصد مشترکی را دنبال می‌کنند.
- فرض ٧: متغیرهای سرعت، سمت، رنج و **CPA** برای تمامی اهداف توسط سامانه رهگیری در اختیار قرار داده شده است.

در ادامه ارکان تهدید برای هر هدف محاسبه شده و میزان امتیاز هر رکن با توجه به فاکتورهای زیر مجموعه‌اش مشخص می‌شود. در نهایت با استفاده از آرایه پنج بعدی تهدید میزان تهدید برای هر هدف تعیین می‌گردد. با تعیین میزان تهدید اختصاص یافته به هر هدف در ادامه لیست اولویت‌بندی شده‌ای از تهدیدات ارائه می‌شود که می‌تواند در مرحله بعد مطابق با شکل (٦) برای برنامه ریزی اقدامات جدید مورد استفاده قرار گیرد. در جدول (٢) و (٣) میزان تهدید اختصاص یافته به هر هدف و میزان امتیاز محاسبه شده برای هریک از ارکان تهدید آورده شده است. میزان تهدید با در نظر گرفتن رکن تحمل‌پذیری در جدول (٢) و بدون در نظر گرفتن آن در جدول (٣) آمده است. چنان که پیداست میزان تهدید و نیز اولویت موجودیت‌های تهدیدی در دو حالت متفاوت هستند. برای بررسی بیشتر و اولویت‌بندی اهداف تهدیدی چنین صحنه ای در اختیار عده‌ای از خبرگان قرار داده شد. تجمیع نظرات این گروه حاکی از عملکرد بهتر رویکرد این پژوهش در اولویت‌بندی تهدیدات دارد.



شکل (۷) : یک صحنه عملیات دریایی و تنوع بازیگران حاضر در آن

۵. نتیجه‌گیری

ارزیابی تهدید از کلیدی‌ترین فرآیندهای سامانه‌های فرماندهی و کنترل به شمار می‌رود به همین جهت وجود سیستم‌های تصمیم‌یار که تحلیل و ارزیابی تهدید را بر عهده دارند می‌تواند در کاهش بار ادراکی اپراتورها بسیار مؤثر باشند. توسعه مفهوم تهدید بر اساس رکنی به نام تحمل‌پذیری در این پژوهش پیشنهاد شد. تحمل‌پذیری جنبه‌ای از حقیقت تهدید را آشکار می‌سازد که در آن هر موجودیتی که در یک موقعیت تاکتیکی قرار می‌گیرد میزان آسیب‌پذیری خود را در برابر اقدامات خودی و واکنش‌های دیگر بازیگران صحنه عملیات تحلیل می‌کند. بر این اساس یک اقدام که از سوی یکی از بازیگران در صحنه عملیات صادر می‌شود می‌تواند برای بازیگران دیگر با توجه به شرایط آن‌ها تهدیدآمیز باشد یا نباشد. وقتی در ارزیابی تهدید برای یک موجودیت در یک موقعیت تاکتیکی میزان قصد، توانمندی و فرصت را در نظر می‌گیریم باید با توجه به گزینه‌های خودی (واکنش در مقابله با تهدید) و هزینه‌های آن را نیز در نظر بگیریم یک اقدام تهدید آمیز در صورتی که گزینه‌های کافی برای مقابله با آن وجود داشته باشد اولویت پایین‌تری را به خود اختصاص می‌دهد در حالی که یک اقدام تهدیدآمیز که گزینه ای برای مقابله با آن در دست نیست و یا هزینه اقدام متقابل نسبت به منافع آن بسیار بالاست اولویت بالایی از تهدید را خواهد داشت. تحمل‌پذیری با آنالیز هزینه‌ها و منافع یک اقدام و همچنین هزینه‌ها و منافع اقدام متقابل آن از سوی بازیگری که اقدام اولیه متوجه آن شده است این مطلب را روشن خواهد ساخت که انجام چنین اقدامی و همچنین تبعات و اثراتی که این اقدام بر موقعیت تاکتیکی و برنامه عملیاتی سایر بازیگران خواهد داشت ارزش آفرینی کافی برای فاعل اقدام را دارد یا خیر. به عبارت بهتر هر بازیگر (دارای عقلانیت) در صحنه عملیات برای دست زدن به یک اقدام باید تحمل اثرات ناشی از اقدام خود را داشته باشد. از این رو اگر بازیگری قصد مشخصی را برای اجرای یک اقدام داشته باشد و توانمندی کافی برای تحقق بخشیدن به قصد خود را نیز داشته باشد و فرصت کافی هم در اختیار داشته باشد اگر قادر به تحمل تبعات اقدام

خود نباشد یا هزینه اقدام او در برابر منافع اقدامش افزون‌تر باشد از دیدگاه عقلانی نمی‌تواند اقدام خود را عملیاتی کند و لذا موقعیت تهدیدی با در نظر گرفتن رکن تحمل‌پذیری متحول خواهد شد. به دنبال توسعه مفهوم تهدید با معرفی رکن تحمل‌پذیری مدلی برای ارزیابی تهدید بر اساس ارکان تشکیل دهنده آن ارائه شد. در این مدل ارکان تهدید با استفاده از شواهدی که حاصل از مشاهده‌گری موقعیت تاکتیکی است تحلیل می‌شوند. شواهد برای تحلیل به صورت گزاره‌هایی منطقی که مقادیری گسسته دارند شکل یافته بودند. این سیستم میزان تهدید هر یک از بازیگران حاضر در صحنه نبرد را ارزیابی کرده و به هر موجودیت یک مقدار عددی نسبت می‌دهد. سپس اهداف مختلف در صحنه عملیات بر اساس میزان تهدید اولویت‌بندی شده و می‌توان بر اساس آن برای اقدامات و واکنش‌های بعدی برنامه‌ریزی و تصمیم‌گیری کرد. سیستم تصمیم‌یار ارزیاب تهدید سپس توسط یک سناریو نبرد دریایی مورد آزمایش قرار گرفت.

مشخص شد که اولویت‌بندی تهدیدات با در نظر گرفتن رکن تحمل‌پذیری تغییرات زیادی را خواهد داشت. خروجی سیستم ارزیاب تهدید که تحمل‌پذیری نیز در آن گنجانده شده عقلانیت بیشتری را در تبیین تهدیدات و اولویت آن‌ها نشان می‌دهد. افزایش تعداد شواهدی که مبنای تحلیل ارکان تهدید هستند می‌تواند به دقیق‌تر شدن محاسبه تهدید بیانجامد بنابراین می‌توان طراحی گزاره‌های بیشتر را در آینده در نظر گرفت. دسته‌بندی شواهد ارزیاب تهدید به نوعی که بتوان برتری برخی شواهد بر شواهد دیگر را در نظر گرفت در دنباله این پژوهش پی گیری خواهد شد.

سپاسگزاری

نویسندگان این مقاله از هم‌فکری‌ها و همکاری‌های ارزشمند اعضای کمیته علمی سازمان صنایع دریایی کمال سپاسگزاری را دارند.

جدول (۲) : امتیازدهی ارکان تهدید برای هریک از اهداف در سناریوی دریایی با در نظر گرفتن تحمل‌پذیری

Target type	Threat element scoring					Calculated threat value	Threat level (rank)
	Proximity	Capability	Intent	Tolerability	Opportunity		
Fighter squadron	1	0.928	0.986	0.5	1	0.882	1
Missile	1	0.75	0.667	0.75	1	0.833	2
Fighter	0.85	0.75	0.861	0.625	1	0.817	3
Frigate	0.7	0.857	0.719	0.625	0.75	0.730	4
Submarine	0.550	0.821	0.708	0.687	0.821	0.717	5
Bomber	0.5	0.821	0.772	0.562	0.964	0.714	6
Group of high speed Boat	0.750	0.624	0.694	0.687	0.785	0.712	7
Helicopter	0.75	0.571	0.763	0.625	0.821	0.706	8
Destroyer	0.300	0.857	0.763	0.5	0.821	0.648	9
AWACS	0.850	0.0.393	0.597	0.375	0.821	0.607	10
Aircraft carrier	0.15	0.821	0.763	0.5	0.678	0.582	11
Passenger airliner	0	0.375	0.277	0.312	0.821	0.353	12

جدول (۳) : امتیازدهی ارکان تهدید برای هریک از اهداف در سناریوی دریایی بدون در نظر گرفتن تحمل‌پذیری

Target type	Threat element scoring				Calculated threat value	Threat level (rank)
	Proximity	Capability	Intent	Opportunity		
Fighter squadron	1	0.928	0.986	1	0.978	1
Fighter	1	0.75	0.667	1	0.865	2
Missile	0.85	0.75	0.861	1	0.854	3
Frigate	0.7	0.857	0.719	0.75	0.756	4
Bomber	0.5	0.821	0.772	0.964	0.751	5
Helicopter	0.75	0.571	0.763	0.821	0.726	6
Submarine	0.550	0.821	0.708	0.821	0.725	7
Group of High speed Boat	0.750	0.624	0.694	0.785	0.718	8
Destroyer	0.300	0.857	0.763	0.821	0.685	9
AWACS	0.850	0.0.393	0.597	0.821	0.665	10
Aircraft carrier	0.15	0.821	0.763	0.678	0.603	11
Passenger airliner	0	0.375	0.277	0.821	0.364	12

٦. مراجع

[1] F. Johansson and G. Falkman, "A Bayesian network approach to threat evaluation with application to an air defense scenario," in 2008 11th International conference on information fusion, 2008, pp. 1-7: IEEE.

[2] H. Irandoust, A. Benaskeur, F. Kabanza, and P. Bellefeuille, "A mixed-initiative advisory system for threat evaluation," in Proceedings of the 15th International Command and Control Research and Technology Symposium: The Evolution of C, 2010, vol. 2, pp. 2-3.

[3] S. Ünver, T. J. J. o. M. Gürbüz, and S. Studies, "Threat Evaluation In Air Defense Systems Using Analytic Network Process," vol. 19, no. 4, 2019.

[4] M. J. Liebhaber and C. Smith, "Naval air defense threat assessment: Cognitive factors and model," PACIFIC SCIENCE AND ENGINEERING GROUP INC SAN DIEGO CA2000.

[5] M. J. Liebhaber and B. Feher, "Air threat assessment: Research, model, and display guidelines," SPACE AND NAVAL WARFARE SYSTEMS COMMAND SAN DIEGO CA2002.

[6] M. J. Liebhaber, D. Kobus, and B. J. S. Feher, "Studies of US Navy air defense threat assessment: Cues, information order, and impact of conflicting data," 2002.

[7] N. Le Guillarme, "A Game-Theoretic Planning Framework for Intentional Threat Assessment," Thèse de doctorat, Université de Caen, 2016.

[8] A. N. Steinberg, "A model for threat assessment," in Fusion Methodologies in Crisis Management: Springer, 2016, pp. 313-340.

[9] E. G. Little and G. L. Rogova, "An ontological analysis of threat and vulnerability," in 2006 9th International Conference on Information Fusion, 2006, pp. 1-8: IEEE.

[10] A. N. Steinberg, "An approach to threat assessment," in 2005 7th International Conference on Information Fusion, 2005, vol. 2, p. 8 pp.: IEEE.

[11] A. N. Steinberg, "Threat assessment technology development," in International and Interdisciplinary Conference on Modeling and Using Context, 2005, pp. 490-500: Springer.

[12] A. N. Steinberg, "Data fusion system engineering," in Proceedings of the Third International Conference on Information Fusion, 2000, vol. 1, pp. MOD5/3-MOD510 vol. 1: IEEE.

[13] J. Llinas, C. Bowman, G. Rogova, A. Steinberg, E. Waltz, and F. White, "Revisiting the JDL data fusion model II," SPACE AND NAVAL WARFARE SYSTEMS COMMAND SAN DIEGO CA2004.

[14] A. N. Steinberg and C. L. Bowman, "Revisions to the JDL data fusion model," in Handbook of multisensor data fusion: CRC Press, 2008, pp. 65-88.

[15] J. Roy, S. Paradis, and M. Allouche, "Threat evaluation for impact assessment in situation analysis systems," in Signal processing, sensor fusion, and target recognition XI, 2002, vol. 4729, pp. 329-341: International Society for Optics and Photonics.

[16] E. Little, G. Rogova, and A. Boury-Brisset, Theoretical foundations and proposed applications of Threat Ontology to information fusion. Defence R&D Canada-Valcartier, 2008.

[17] F. Johansson and G. Falkman, "A comparison between two approaches to threat evaluation in an air defense scenario," in International Conference on Modeling Decisions for Artificial Intelligence, 2008, pp. 110-121: Springer.

[18] N. Okello and G. Thoms, "Threat assessment using Bayesian networks," in Proceedings of the 6th International Conference on Information fusion, 2003, pp. 1102-1109.

[19] Y. Hou, W. Guo, and Z. Zhu, "Threat assessment based on variable parameter dynamic Bayesian network," in Proceedings of the 29th Chinese Control Conference, 2010, pp. 1230-1235: IEEE.

[20] W. Mei, "Air Defense Threat Evaluation using Fuzzy Bayesian Classifier," in IJCCI, 2013, pp. 227-232.

[21] S. Kumar and B. K. J. P. T. Tripathi, "Modelling of threat evaluation for dynamic targets using bayesian network approach," vol. 24, pp. 1268-1275, 2016.

[22] S. F. Page, J. P. Oldfield, and P. Thomas, "Towards integrated threat assessment and sensor management: Bayesian multi-target search," in Multisensor Fusion and Integration for Intelligent Systems (MFI), 2016 IEEE International Conference on, 2016, pp. 44-51: IEEE.

[23] A. N. Costa and P. C. Costa, "Simulation-based air mission evaluation with Bayesian threat assessment for opposing forces," in Disciplinary Convergence in Systems Engineering Research: Springer, 2018, pp. 281-295.

[24] M. Nilsson, J. Van Laere, T. Ziemke, and J. Edlund, "Extracting rules from expert operators to support situation awareness in maritime surveillance," in 2008 11th International conference on information fusion, 2008, pp. 1-8: IEEE.

[25] W. Elahsoumi, I. Boujelben, and I. Keskes, "Rule Based Method for Terrorism, Violence and Threat Classification: Application to Arabic Tweets," in International Conference on Automatic Processing of Natural-Language Electronic Texts with NooJ, 2019, pp. 209-219: Springer.

[26] Y. Liang, J. Lee, B. Hong, and W. Kim, "Design and Implementation of Rule-based CEP for Threat Detection and Defense," in 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), 2019, pp. 1-6: IEEE.

[27] A. N. J. H. o. m. d. f. t. Steinberg and practice, "Foundations of situation and threat assessment," pp. 437-501, 2009.

[28] M. Oxenham, "Enhancing situation awareness for air defence via automated threat analysis," in Proceedings of the Sixth International Conference on Information Fusion, 2003, vol. 2, pp. 1086-1093.

[29] M. G. Oxenham, "Using contextual information for extracting air target behavior from sensor tracks," in Signal Processing, Sensor Fusion, and Target Recognition XII, 2003, vol. 5096, pp. 482-493: International Society for Optics and Photonics.

[30] Y. Liang, "An approximate reasoning model for situation and threat assessment," in Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007), 2007, vol. 4, pp. 246-250: IEEE.

[31] C. Giraud and B. Jouvencel, "Sensor selection in a fusion process: a fuzzy approach," in Multisensor Fusion and Integration for Intelligent Systems, 1994. IEEE International Conference on MFI'94., 1994, pp. 599-606: IEEE.

[32] S. Kumar and A. M. Dixit, "Threat evaluation modelling for dynamic targets using fuzzy logic approach," in International Conference on Computer Science and Engineering, 2012.

[33] E. Azimirad, J. J. I. J. o. C. S. Haddadnia, and I. Security, "A New Data Fusion Instrument for Threat Evaluation Using of Fuzzy Sets Theory," vol. 13, no. 4, p. 19, 2015.

[34] E. Azimirad and J. J. I. J. o. A. i. I. I. Haddadnia, "A New Method for Threat Assessment Based on Fuzzy Dempster-shaffer Theory," vol. 2, no. 2, pp. 54-64, 2016.

[35] E. Azimirad and J. J. I. J. o. A. i. I. I. Haddadnia, "A new model for threat assessment in data fusion based on fuzzy evidence theory," vol. 2, no. 2, pp. 54-64, 2016.

[36] B. J. Choi, J. E. Kim, J. S. Kim, C. O. J. J. o. t. K. I. o. M. S. Kim, and Technology, "Fuzzy rule-based method for air threat evaluation," vol. 19, no. 1, pp. 57-65, 2016.

[37] M. J. Liebhaber and B. Feher, "Surface warfare threat assessment: Requirements definition," SPACE AND NAVAL WARFARE SYSTEMS COMMANDSAN DIEGO CA2002.

[38] S. You, M. Diao, L. J. I. R. Gao, Sonar, and Navigation, "Implementation of a combinatorial-optimisation-based threat evaluation and jamming allocation system," vol. 13, no. 10, pp. 1636-1645, 2019.

[39] L.-b. QIU, Z.-l. LIU, and M. J. J. o. A. F. E. U. LIU, "A Threat Assessment Algorithm by Using the Neural Network Techniques [J]," vol. 6, 2002.

[40] X. Ximeng, Y. Rennong, and Y. Yang, "Threat Assessment in Air Combat Based on ELM Neural Network," in 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), 2019, pp. 114-120: IEEE.

[41] S.-l. Zhang, T. Zhang, and X.-m. Xu, "Threat Estimation of Aerial Target Based on Extreme Learning Machine," in 2019 Chinese Control Conference (CCC), 2019, pp. 7233-7238: IEEE.

[42] H. Lee, B. J. Choi, C. O. Kim, J. S. Kim, and J. E. J. K.-B. S. Kim, "Threat evaluation of enemy air fighters via neural network-based Markov chain modeling," vol. 116, pp. 49-57, 2017.

[43] A. Benavoli, B. Ristic, A. Farina, M. Oxenham, and L. Chisci, "An approach to threat assessment based on evidential networks," in 2007 10th International Conference on Information Fusion, 2007, pp. 1-8: IEEE.

[44] R. Roux and J. H. J. O. van Vuuren, "Real-time threat evaluation in a ground based air defence environment," vol. 24, no. 1, pp. 75-101, 2008.

[45] M. Yoon, J. Park, and J. J. I. J. o. C. Yi, "An Effective Threat Evaluation Algorithm for Multiple Ground Targets in Multi-target and Multi-weapon Environments," vol. 15, no. 1, 2019.

[46] I. Dimitrijević and N. Stekić, "Intelligence Analysis Models for Asymmetric Threats," Strategic Research Institute & National Defence School, 2018.

[47] G. Rogova and P. Scott, Fusion Methodologies in Crisis Management: Higher Level Fusion and Decision Making. Springer, 2016.