



## Prioritized Solutions of Electronic and Cyber Defense in Drone Detection and Defense using Analytical Hierarchy Process (AHP)

Mojtaba Araghzadeh<sup>a</sup>, Gholam Reza Jalali Farahani<sup>b</sup>, Foruzan, Hamid<sup>c</sup>

<sup>a</sup>Passive Defense Faculty of Malek Ashtar University of Technology, Tehran, Iran

<sup>b</sup>Supreme National Defense University, Tehran, Iran

<sup>c</sup>Department of Passive Defense Strategic Management, Supreme National Defense University, Tehran, Iran

### ARTICLE INFO

### ABSTRACT

#### Keywords:

Analytic Hierarchy Process, Drone Threats, Detection, Defense, Electronic Defense, Cyber Defense

Drones now have many useful functions, ranging from monitoring pipelines, photography, filming, and as a hobby for teenagers. Despite diversity of civil and military uses of drones for countries, they have threats for critical infrastructures and key assets. Nowadays, they are used beside war fighter planes. Drone attacks can be done by commercial drones dropping bombs, firing a missile, or crashing into a target. One of the main concerns is the unauthorized use of drones near critical infrastructure, public events, and sensitive locations. For instance, drones flying near airports or nuclear power plants pose a serious threat to security. Unauthorized drone activities can interfere with operations, compromise safety, and even facilitate criminal acts. Furthermore, because of their high efficiency and low cost among manned planes, they are more favorable for world armies. The availability of advanced navigation and satellite communication technologies has revolutionized the use of drones, making them more versatile. They can now endure missions by 40 hours, far beyond the capabilities of human crew. With in-flight refueling and ultra-efficient solar power, the drones can provide an even greater range of operation. Meanwhile, in order to deter drone threats, diverse actions have done in the world, called "Counter-drone technologies or systems". Counter-drone technology encompasses a wide range of ways that allow you to detect, classify, and mitigate unmanned aerial vehicles. Parallel of using drones in the world, developing of counter-drone technologies is on process. More of these technologies are based on electronic and cyber defense methods.

#### Received:

10 May 2024

#### Received in revised form:

05 July 2024

#### Accepted:

24 July 2024

pp. 153-169

Corresponding author (Email: [mojtabarezvani313@gmail.com](mailto:mojtabarezvani313@gmail.com))

Copyright © 2022 The Authors. Published by Passive Defense Association of Iran. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>).

The growth of counter-drone technology is related to the increase in concerns about the threat that drones pose to civilian and military infrastructures. Counter drone systems have become essential for the safety and security of critical infrastructures. Counter-drone systems detect and intercept the unknown drones by taking into account their flight path, physical properties such as size and kinetic energy, the number of swarming drones, and the likely damage which could be caused. Counter-drone systems are fixed or preferably portable and have the capability of defending the facilities like military establishments and sites, airports, petroleum facilities, etc. by quickly detecting multiple drones at sufficient distances.

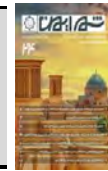
Drone detection technology works to detect drones in the airspace. The most popular ways to detect drones electronic and cyber defense are: acoustic sensors, electro-optical and infra-red sensors, RADAR and radio frequency sensors. Acoustic sensors can involve one or multiple microphones and software. These technologies can detect drones by engine sound to calculate distance and direction. Optical sensors (cameras) utilize multiple wavelengths (thermal, infrared, etc.) for day or night drone detection, and the technology is evolving quickly to extend range and intelligence with AI capabilities. Radar uses radio waves to determine distance and speed of objects. It is accurate and identifies hundreds of targets simultaneously, including all drone types (piloted or autonomous) in many weather conditions. RF sensors consist of one or multiple antennas of various ranges to detect communications between and drone and its controller (human operator). Although for drone mitigation or interception, the best are electromagnetic pulse (EMP) or high power microwave (HPM), laser guns, electromagnetic field, jamming and spoofing.

This research aimed to develop prioritized solutions of electronic and cyber defense in drone detection and defense.

In this research, which is applicable in nature, the most popular methods in electronic and cyber defense were identified and analyzed using of a mixed methodology after a literature review on drone detection and defense systems. Then by using of library studies and expert opinions, 11 criteria were gathered and prioritized using AHP method. These 11 criteria were: response time, cost, side-effects, operator skills, ability to detect autonomous drones, range, accuracy, intensity of effect, ability to drone landing, ability to build in the country, accessibility to system details.

In this process, it was known that performance accuracy and functional range of detection systems have the best points. Then each of drone detection and defense was marked and by multiplying scores in weight of each criterion, final scores of each drone detection and defense system was identified in order to prioritize them.

At last, it became clear that for drone detection based on determined criteria the best method is RADAR based method and for defense is HPM. Thus, using of laser systems and cyber spoofing with a slight difference were on next steps of drone defense.



## راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهبادی با استفاده از روش تحلیل سلسله‌مراتبی

مجتبی عراقی زاده\*، غلامرضا جلالی فراهانی، حمید فروزان

- ۱- پژوهشیارمجمع دانشگاهی مهندسی و پدافند غیر عامل
- ۲- دانشیار دانشگاه عالی دفاع ملی
- ۳- استادیار گروه مدیریت راهبردی دانشگاه عالی دفاع ملی

### چکیده

پژوهش حاضر با هدف ارائه راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری برای شناسایی و مقابله با تهدیدات پهبادی به انجام رسیده است. در پژوهش حاضر که از نظر ماهیت، کاربردی می‌باشد با بهره‌گیری از روشی ترکیبی پس از یک مطالعه مروری بر روی روش‌های شناسایی و مقابله با تهدیدات پهبادی، مرسوم‌ترین این روش‌ها از جدیدترین منابع شناسایی و ارزیابی گردیدند. در ادامه با بهره‌گیری از مطالعات کتابخانه‌ای و نظر خبرگان، ۱۱ معیار برای رتبه‌بندی این روش‌ها احصاء و با روش تحلیل سلسله‌مراتبی رتبه‌بندی گردیدند. سپس هریک از روش‌های شناسایی و مقابله بر اساس معیارهای شناسایی شده بر اساس

### واژگان کلیدی

تحلیل سلسله‌مراتبی،  
تهدیدات پهبادی،  
شناسایی، مقابله،  
پدافند الکترونیک،  
پدافند سایبری

ویژگی‌ها و محدودیت‌های احصاء شده در بخش ادبیات پژوهش برای هریک از روش‌های شناسایی و مقابله با تهدیدات پهبادی، نمره‌گذاری گردیدند و با ضرب نمودن امتیازهای به‌دست‌آمده در وزن هر معیار، امتیاز نهایی هریک از روش‌های شناسایی و مقابله با تهدیدات پهبادی حاصل گردید تا از این طریق بتوان آنها را رتبه‌بندی نمود. در پایان مشخص گردید برای شناسایی پهبادها، بهترین روش بر اساس معیارهای تعیین شده، روش‌های مبتنی بر سامانه‌های راداری بوده و برای مقابله با پهبادها، بهترین روش، بهره‌گیری از پالس الکترومغناطیسی می‌باشد. همچنین بهره‌گیری از سامانه‌های لیزری و ایجاد فریب سایبری برای پهباد با اختلاف ناچیزی در رتبه بعدی روش‌های مقابله با تهدیدات پهبادی قرار گرفتند.

پژوهشگاه علوم انسانی و مطالعات فرهنگی  
پرتال جامع علوم انسانی

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهن‌بند با استفاده از روش تحلیل سلسله‌مراتبی

## ۱- کلیات

### ۱-۱- طرح مسئله

گسترش روزافزون دامنه تهدیدات پهن‌بندهای جاسوسی و تهاجمی علیه منافع ملی کشور توسط کشورهای فرامنطقه‌ای ایجاب می‌کند که نظام دفاعی کشور برای مقابله با آنها به بازبینی و بهینه‌سازی فرایندهای عملیاتی خود در این زمینه بپردازد (حبیبی، ۱۳۹۳: سخن‌آغازین). علت توجه به پرنده‌های بدون سرنشین این است که در بخش‌های نظامی، از آن زمان که بشر خود را شناخته، از جنگ تن‌به‌تن و گلاویز شدن دوری کرده است و لذا به‌طور تدریجی با ابداع ابزارها، فاصله انسان‌ها را در جنگ‌ها از یکدیگر بیشتر کرده است و این روند افزایش فاصله بین دو جبهه درگیری، یک اصل ثابت بوده است (رستمی، ۱۳۹۱). به‌علاوه، کارایی و اثربخشی هواپیماهای بدون سرنشین با توجه به توانمندی بسیار بالای آنها و سهولت کاربری، نگهداری، ساخت و تولید و همچنین ارزان‌قیمت بودن در مقایسه با هواپیماهای سرنشین‌دار، مورد توجه ارتش‌های جهان قرار گرفته است (شکوهی، ۱۳۹۲: ۱۳).

با وجود آنکه پهپادها کاربردهای نظامی و غیرنظامی بسیار مفیدی برای کشورها دارند و از سالیان پیش کاربردهای متعددی برای پهپادها در حوزه تجاری مطرح بوده است (کاظمی و الهیان، ۱۳۹۹: ۴۸)، اما به‌موازات بهره‌گیری از منافع، تهدیدات آنها نیز به‌شدت علیه دارایی‌ها و زیرساخت‌های کشورها گسترش یافته است. در واقع در جنگ‌های آینده ترکیبی از هواپیماهای با سرنشین و بدون سرنشین به‌کار گرفته خواهد شد (حبیبی، ۱۳۹۳: مقدمه). پهپادها دسته‌بندی‌های گوناگونی دارند که مهم‌ترین و رایج‌ترین دسته‌بندی پهپادها در جهان عبارتند از دسته‌بندی بر اساس اندازه و وزن، دسته‌بندی بر اساس چگونگی کنترل پرواز و دسته‌بندی بر اساس نوع مأموریت پهپاد (خرم‌فعال، ۱۳۹۹: ۱۷). بر اساس اندازه و وزن به سه دسته راهبردی،

عملیاتی و تاکتیکی، بر اساس چگونگی کنترل پرواز سه دسته پیش‌برنامه‌ریزی‌شده، کنترل از راه دور و کنترل بر اساس هوش مصنوعی و بر اساس نوع مأموریت به پنج دسته شناسایی، مراقبت، انتحاری، تهاجمی و هدف‌تقسیم‌بندی می‌شوند (همان: ۵۶).

در این میان برای مقابله با تهدیدات پهن‌بند اقدامات مختلفی در دنیا تحت عنوان فناوری‌های ضد پهپاد صورت گرفته است. فناوری ضد پهپاد که به‌عنوان فناوری ضد سامانه‌های بدون سرنشین نیز شناخته می‌شوند به سامانه‌هایی اشاره دارند که برای شناسایی و یا رهگیری هواپیماهای بدون سرنشین استفاده می‌شوند. درحالی‌که نگرانی از تهدیدهای امنیتی بالقوه از پهپادهای نظامی و نیز شخصی در حال رشد است یک بازار جدید برای فناوری ضد پهپاد به‌سرعت در حال ظهور است. تا به امروز حداقل ۲۳۵ عدد از محصولات ضد پهپاد در بازار و یا در حال تحقیق و توسعه برای ورود به بازار شناسایی شده‌اند (هالند (Holland)، ۲۰۱۸: ۱) به نقل از (پدرام و همکاران، ۱۳۹۷: ۱۴۷). این روش‌ها عمدتاً مبتنی بر پدافند الکترونیک و پدافند سایبری هستند. از جمله سامانه‌هایی که به‌عنوان آشکارساز و رهگیر پهپاد می‌توان به آنها اشاره کرد عبارتند از: رادار، امواج رادیویی، تصویری، مادون‌قرمز، صوتی و حسگرهای ترکیبی؛ بنابراین مسئله پژوهش حاضر، اولویت‌بندی راهکارهای شناسایی و مقابله با تهدیدات پهن‌بند چگونه می‌باشد.

### ۱-۲- محدودیت‌های تحقیق

از آنجاکه این حوزه جزو حوزه‌های لبه‌دانشی و نوین در عرصه علوم نظامی می‌باشد، داده‌ها و اطلاعات به‌کار برده شده در این پژوهش از میان آخرین منابع در دسترس در بسترهای علمی گردآوری گردید. طبیعتاً ممکن است روش‌هایی و روش‌های ذکر شده در این پژوهش وجود

داشته باشد که هنوز به عرصه عمومی معرفی نشده باشند.

### ۱-۳- پیشینه و ادبیات موضوع

جنگ الکترونیک و جنگ سایبری در حال تبدیل شدن به عناصر کلیدی صحنه نبرد هستند، به خصوص زمانی که عملیات نظامی وابستگی بیشتری به تفوق اطلاعاتی داشته باشد. تسلط بر طیف الکترومغناطیسی و سامانه‌های اطلاعاتی، فرمانروایی مطلق در میدان جنگ را به ارمغان خواهد آورد و مخاطرات ناشی از وابستگی عناصر صحنه نبرد به شبکه‌های ارتباطی و سامانه‌های اطلاعاتی را کاهش می‌دهد. وجوه اشتراکات جنگ سایبری و جنگ الکترونیک در اصول و فرآیند اجرا و همچنین تأثیرات و پیامدهای نسبتاً مشابه آنها در سازمان‌های نظامی، سبب همگرایی بین دو عرصه شده است. استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برتری‌ساز و تعیین کننده در نبردهای آینده خواهد بود. کشورهای بهره‌مند از این دو عامل قادر خواهند بود تا نبردها را با حداقل تلفات انسانی و کمترین هزینه به نفع خود به پایان برسانند (فرحخت و دهقانی، ۱۳۹۸:۲۰۰).

در سال‌های اخیر توجه به روش‌های شناسایی و مقابله با تهدیدات پهنادای به روش‌های پدافند الکترونیک و پدافند سایبری بسیار مورد توجه قرار گرفته است. چیپر (*Chiper*) و همکاران (۲۰۲۲) در مقاله‌ای مروری و ارزشمند، با بررسی ۱۸۶ منبع علمی در رابطه با روش‌های شناسایی و مقابله با این تهدیدات پرداخته‌اند. آنها معتبرترین روش‌ها را شناسایی کرده و به بیان ویژگی‌ها و نقاط ضعف هریک از روش‌ها پرداخته‌اند و در انتها سامانه پیشنهادی خود را معرفی کرده‌اند (چیپر و همکاران، ۲۰۲۲). پدرا و همکاران نیز (۱۳۹۸) در پژوهشی با عنوان آینده پژوهی در حوزه محصولات ضد پهناد با استفاده از اولویت‌گذاری پابرجا پس از معرفی روش‌ها و فناوری‌های مختلف ضد پهناد و ارائه نقاط مثبت و

منفی آنها، تلاش نموده‌اند با روشی جدید، نسبت به اولویت‌گذاری فناوری‌های آتی در این حوزه تمرکز داشته باشند و به این ترتیب رویکردهای پیشنهادی خود را در زمینه محصولات ضد پهناد بیان کرده‌اند. در این پژوهش تفکیک مابین روش‌های سخت مقابله و روش‌های پدافند الکترونیک و سایبری صورت پذیرفته است (احمدیان و مزلقانی، ۱۳۹۷). کراتکی (*Kratky*) و فارلیک (*Farlik*) (۲۰۱۸) در مقاله‌ای مقابله با پهنادها- جلورنده تحقیقات در فناوری‌های نظامی که با هدف تأکید بر ایجاد زمینه‌های علمی جدید در ارتباط با فناوری‌های ضد پهناد به انجام رسیده است، به بیان رشته‌ها و حوزه‌های علمی که باید در ارتباط با مقابله با پهناد فعال شده و می‌توانند اقدامات مؤثری انجام دهند، پرداخته‌اند. در ادامه نیز مهم‌ترین فناوری‌های شناسایی و مقابله را معرفی کرده‌اند اما بیشترین تأکید این مقاله بر لزوم آغاز یک حرکت علمی وسیع در زمینه مقابله با تهدیدات پهناد است (کراتکی و فارلیک، ۲۰۱۸). براست (*Brust*) و همکاران (۲۰۱۸) در پژوهشی با عنوان دفاع در برابر نفوذ پهنادهای مهاجم با استفاده از شبکه‌ای از پهنادهای دفاعی به ارائه راه‌حلی خلاقانه برای مقابله با تهدیدات پرداخته‌اند که طی آن به مجرد تشخیص نزدیک شدن پهناد مهاجم، شبکه‌ای منسجم از پهنادهای مدافع اقدام به محاصره پهناد مهاجم از سه جهت نموده و امکان حرکت را از آن سلب می‌نمایند و در نهایت نیز آن پهناد را به خارج از محیط حفاظت‌شده هدایت می‌کنند. این روش از الگوریتم‌های خاص و پیچیده‌ای برای شناسایی، محاصره و هدایت جهت‌دار پهناد مهاجم بهره برده و امکان و هزینه‌های پیاده‌سازی آن برای زیرساخت‌های مختلف باید مورد بررسی قرار گیرد (براست و همکاران، ۲۰۱۸). فارلیک و همکاران (۲۰۱۹) در مقاله‌ای با عنوان شناسایی چند طیفی پهنادهای تجاری که حاصل کار پژوهشی چهار سال‌های بوده است روش‌های شناسایی پهنادها بر اساس طیف‌های مختلف

- زمین پایه متحرک (روی خودرو)
- دستی (قابل حمل با دست)
- نصب‌شده بر روی یک پهپاد
- نصب‌شده بر روی چند پهپاد

#### ۱-۵- انواع فناوری‌های شناسایی

از مهم‌ترین فناوری‌های شناسایی پهنپادهای مهاجم می‌توان به موارد زیر اشاره کرد:

#### ۱-۵-۱- آکوستیک (صوتی)

حسگرهای آکوستیک یکی از گزینه‌های مطرح برای کشف ریزپرنده‌ها هستند این حسگرها به صداهای محیطی گوش می‌دهند و صدای خاص ریز پرنده‌ها را از میان صداهای موجود تشخیص می‌دهند. حسگر به محض آنکه صدایی را می‌شنود آن را با صداهای موجود در بانک داده خود مقایسه می‌کنند تا صدای ریز پرنده را شناسایی و نوع پرنده را تشخیص دهد. در این حالت هشدار امنیتی برای عوامل مربوطه صادر می‌شود. در شرایطی که رادارهای فعال و غیرفعال ناکارآمد هستند می‌توان از حسگرهای آکوستیک در این خصوص استفاده کرد. این حسگرها مقرون‌به‌صرفه بوده و کار با آنها ساده است، البته این حسگرها به‌عنوان تنها گزینه نباید به کار روند و همواره باید در ترکیبی از گزینه‌ها به کار گرفته شوند. چالش‌های پیش روی حسگرهای آکوستیک در این است که باید مبتنی بر بانک داده فعالیت کنند و چنانچه کتابخانه داده آنها به‌روز نباشد قادر به کشف ریز پرنده نخواهند بود در نتیجه به‌روزرسانی کتابخانه حسگر آکوستیک با صداهای ریزپرنده در صنعتی که هر روز نوآوری دارد یک چالش اساسی است که هیچ‌گاه به پوشش ۱۰۰٪ نمی‌رسد (کافی، ۱۴۰۰: ۲۲۰). این فناوری حاوی آرایه‌ای از میکروفون‌ها هستند که پایگاه داده‌ای از صداهای تولیدی از روتورهای پهپادها را دارند و با مقایسه صدای پهنپادهای

الکترومغناطیسی را تحلیل کرده‌اند و راه‌حل‌های راداری را برای شناسایی پهنپادهای مناسب دانسته‌اند. هرچند به این مسئله نیز اذعان کرده‌اند که هیچ راه‌حل جامع و کاملی برای شناسایی پهنپادهای وجود ندارد و باید مطالعات بسیار بیشتری در این زمینه صورت پذیرد (فارلیک و همکاران، ۲۰۱۹). همچنین نوروزی (۱۳۹۴) در مقاله‌ای با عنوان بررسی حملات الکترونیک علیه پهپادها، حملات الکترونیک علیه سیستم‌های ارتباط رادیویی، ماهواره‌ای و شبکه ارتباطی پهپادها را مورد بررسی قرار داده و راهکارهای متناسب هریک از حملات را پیشنهاد داده است. در این مقاله علاوه بر حملات الکترونیکی علیه پهپادها، حملات سایبری علیه آنها نیز به دو شکل سخت‌افزاری و نرم‌افزاری مورد توجه قرار گرفته است (نوروزی، ۱۳۹۴)، لکن در این مقاله نیز مانند مقالات یاد شده پیشین موضوع اولویت‌بندی و رتبه‌بندی روش‌های دفاع الکترونیک و سایبری در برابر تهدیدات پهنپایه رخ نداده است.

آنچه به‌عنوان جمع‌بندی از پیشنهادها ذکر شده در این مقاله و سایر پیشنهادهایی که از ذکر آنها صرف‌نظر شده است حاصل می‌شود این است که فناوری‌های متعدد شناسایی و مقابله با تهدیدات پهنپایه به‌خوبی شناسایی و معرفی شده‌اند و مزایا و معایب هر یک نیز بیان گردیده‌اند اما با توجه به اینکه هر یک از روش‌های یاد شده از مزایا و معایبی برخوردار هستند، نوعی و اولویت‌بندی برای انتخاب سامانه برتر شناسایی و مقابله با تهدیدات پهنپایه به انجام نرسیده است. به‌عبارت‌دیگر انتخاب سامانه برای انتخاب‌گران غیرحرفه‌ای در شرایط فعلی دشوار است که این مقاله به دنبال برطرف نمودن این چالش است.

#### ۱-۴- انواع سیستم‌های شناسایی و دفاع در برابر تهدیدات پهنپایه از نظر محل قرارگیری

- زمین پایه ثابت



برای انتخاب رادار کشف باید ملاحظات زیر را در نظر گرفت: (کافی، ۲۱۹:۱۴۰۰)

- مسافت مورد نیاز برای کشف
- مکان به کارگیری رادار
- ابعاد دارایی مورد پوشش
- درجه اهمیت دارایی مورد پوشش به منظور تعیین هزینه‌های قابل قبول

می‌توان از ترکیبی از رادارهای فعال و غیرفعال استفاده کرد. رادارهای فعال به عنوان گیرنده امواج پراکنده در فضا مانند امواج مخابراتی عمل می‌کنند و از نظر هزینه ابعاد قطعات مکانیکی و نیازهای تعمیراتی در مقایسه با رادارهای فعال در مرتبه پایین‌تری قرار دارند.

#### ۱-۵-۴- تحلیل گر امواج رادیویی (RF)

برای کشف ریزپرنده‌ها از سامانه فرکانس رادیویی مانند تحلیلگر طیف فرکانس رادیویی و یا نرم‌افزار استفاده می‌شود تا طیف فرکانسی پرنده کشف شود و لینک بین فرماندهی و کنترل و پرنده و لینک بارگذاری ویدیو مشخص شود. با کشف و لینک فرکانس رادیویی می‌توان به سایر اطلاعات مانند سازنده و پرنده و یا نوع آن پی برد. این اطلاعات در ارزیابی تحلیل بسیار مفید است. بسیاری از سامانه‌های فرکانس رادیویی تنها قادر به کشف پرنده هستند اما با اتکال به راه‌حل‌های فناورانه مانند استفاده از آنتن‌های مولتی استاتیک متعدد می‌توان اطلاعات کاملی شامل مثلث جغرافیایی پرنده و موقعیت کاربر را مشخص نمود (کافی، ۲۱۸:۱۴۰۰).

این تحلیل‌گرها شامل یک یا چند آنتن برای دریافت امواج رادیویی است و یک پردازشگر نیز برای تحلیل طیف-های فرکانس‌های رادیویی دارد. در این روش از فرکانس‌های رادیویی (RF) میان پهپاد و پایگاه کنترل آن استفاده می‌شود و سیگنال‌های انتقالی میان پهپاد و کنترل‌کننده آن

نزدیک‌شونده با این پایگاه داده، حضور آنها را تشخیص می‌دهند (چیپر و همکاران، ۲۰۲۲:۷). برای شناسایی محل پهپاد به تعداد بیشتری از این میکروفون‌ها نیاز است (همینگا و همکاران: ۲۰۲۲).

#### ۱-۵-۲- سنجنده‌های تصویربرداری

این سنجنده‌ها شامل دو نوع دوربین الکترواپتیکال (EO) و مادون‌قرمز (IR) هستند.

- دوربین اپتیکی (EO): این نوع سنجنده‌ها را می‌توان در کنار سایر سنجنده‌ها نظیر رادار و RF نیز به کار برد و با گرفتن تصویر پهپاد، ویژگی‌های آن را تعیین کرد. بزرگ‌ترین مشکل این سنجنده‌ها آن است که در محیط‌های تاریک و مه‌آلود قابلیت استفاده پایینی دارند. به علاوه کیفیت تصاویر بستگی دارد به کیفیت لنزها و زاویه تصویربرداری (نیاز ضروری به خط دید).
- دوربین حرارتی: در این روش بر اساس حرارت تولید شده از موتور، باتری و پردازنده‌ها پهپاد شناسایی می‌شود. این روش محدودیت‌هایی شامل محدوده پایین شناسایی و حساسیت‌های محیطی که امکان تشخیص اختلاف دمای پهپاد و محیط اطراف را به وجود می‌آورد، دارد.

#### ۱-۵-۳- رادار (شناسایی بر اساس سطح مقطع راداری)

سامانه‌ای است که از امواج راداری برای شناسایی اشیاء استفاده می‌کند. رادار یک سیگنال ارسال و بازگشت آن را دریافت می‌کند و از این طریق، جهت حرکت، فاصله و موقعیت پهپاد را تعیین می‌کند. بیشتر رادارها برای شناسایی اهداف بزرگ مقیاس طراحی شده‌اند و توانایی تشخیص پرنده‌های کوچک را ندارند. راه‌حل راداری یک راه‌حل اکتیو یا عامل است که می‌توان با استفاده از آن، محدوده، زاویه و سرعت پهپاد را شناسایی کرد. رادار شامل فرستنده، گیرنده و پردازنده است (همینگا و همکاران: ۲۰۲۲).

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهنای با استفاده از روش تحلیل سلسله‌مراتبی

قوی برای ایجاد یک میدان مغناطیسی که دور کننده پهنایها می‌باشد استفاده می‌شود (چیپر و همکاران، ۲۰۲۲: ۸).

#### ۱-۶-۴- جمر با فرکانس رادیویی (RF/GSNS)

جمر با فرکانس رادیویی وسیله‌ای قابل حمل است که حجم بالایی از امواج رادیویی را از خود ساطع می‌کند و به سمت هدف می‌تاباند و با این کار، سیگنال‌های مابین کنترل کننده پهنای و خود پهنای را مورد اختلال و پوشش قرار می‌دهد. در چنین شرایطی یکی از چهار حالت زیر پدید می‌آید:

- پهنای یک فرود کنترل شده در موقعیت خود خواهد داشت

- پهنای به سمت موقعیت از پیش تعیین شده‌اش بازمی‌گردد. (این موقعیت ممکن است موقعیت هدف مورد نظر باشد نه مبدأ اصلی)

- به شکل غیرکنترل شده‌ای به زمین می‌افتد.

- به سمت نامعلومی به شکل غیرکنترل شده‌ای به پرواز درمی‌آید.

#### ۱-۶-۵- فریب‌دهنده‌های سامانه موقعیت‌یاب جهانی

##### (GPS Spoofer)

این سامانه، سیگنال جدیدی را به سمت پهنای می‌فرستد که ارتباط میان سامانه موقعیت‌یاب جهانی (GPS) و ماهواره را جایگزین می‌کند و با این کار، پهنای دچار فریب شده و به مکان دیگری می‌رود. با تغییر دائمی مختصات جی‌پی‌اس پهنای به صورت در لحظه، موقعیت پهنای توسط فریب‌دهنده کنترل می‌شود و بنابراین می‌توان پهنای را در نقطه مطلوب فرود آورد (همینگا و همکاران: ۲۰۲۲).

#### ۱-۶-۶- ترکیبی

در این روش، ترکیبی از سامانه‌های یاد شده مورد استفاده و بهره‌برداری قرار می‌گیرند

شناسایی و تحلیل می‌شود. این سیگنال‌ها گاهی بالارونده و گاهی پایین‌رونده هستند (همینگا و همکاران: ۲۰۲۲).

#### ۱-۵-۵- ترکیبی

#### ۱-۶-۶- مهم‌ترین روش‌های مقابله یا سرنگونی

##### پدافند الکترونیک و پدافند سایبری

مهم‌ترین روش‌های مقابله یا سرنگونی پهنایهای مهاجم عبارتند از:

#### ۱-۶-۱- پالس الکترومغناطیسی (EMP)

این سامانه‌ها، پالس الکترومغناطیسی تولید می‌کنند که می‌تواند در تجهیزات الکترومغناطیسی اختلال به وجود آورد. پالس‌های الکترومغناطیسی با لینک‌های رادیویی ایجاد اختلال نموده و گاهی مدارهای الکترونیکی پهنای را از بین می‌برد. (حتی ممکن است مدارات سایر تجهیزات الکترونیکی پیرامونی را به خاطر ولتاژهای مخرب بالا و جریان‌های الکتریکی زیادی که به وجود می‌آورند از بین ببرد).

سامانه‌های امواج ماکروویو با انرژی بالا (HPM) ممکن است شامل آنتنی برای متمرکز کردن پالس‌های الکترومغناطیسی در یک جهت مشخص با هدف کاهش پیامدهای جانبی داشته باشد (همینگا و همکاران: ۲۰۲۲).

#### ۱-۶-۲- لیزر

سامانه‌ای اپتیکی با انرژی بالا که پرتو نور پر انرژی تولید کرده و می‌تواند آسیب جدی به ساختار پهنای و مدارات الکترونیکی آن وارد نماید.

#### ۱-۶-۳- ایجاد میدان مغناطیسی

این روش به تازگی توسط مجموعه‌ای در کشور امارات متحده عربی به کار گرفته شده است که طی آن از آهن‌رباهای بسیار



جدول ۱- ویژگی‌ها و محدودیت‌های روش‌های شناسایی پهبادهای (چپیر و همکاران، ۲۰۲۲)، (همینگا و همکاران، ۲۰۲۲)، (پدرام مزلقانی و همکاران، ۱۳۹۵) (تجمیع و گردآوری شده توسط نگارندگان، ۱۴۰۲)

روش	ویژگی‌ها	محدودیت‌ها
اکوستیک (صوتی)	<ul style="list-style-type: none"> <li>- از طیف ۲۰ هرتز تا ۲۰ کیلوهرتز را پوشش می‌دهد.</li> <li>- پایگاه داده علائم صوتی دستگاه به راحتی قابل به روزرسانی است.</li> <li>- سبک وزن است و به راحتی می‌توان از آن در کنار سایر سنجنده‌ها بهره برد.</li> <li>- توانایی شناسایی پهبادهای خودکار و غیرخودکار را در ارتفاع پایین دارند.</li> <li>- در محیط‌های ناهموار می‌توان آنها را قرار داد و از آنها استفاده کرد.</li> <li>- به صورت غیرفعال (پسیو) عمل می‌کنند.</li> </ul>	<ul style="list-style-type: none"> <li>- برد محدود</li> <li>- آسیب‌پذیر در برابر نویزهای محیط (در محیط‌های پر نویز جوابگو نیستند)</li> <li>- مستعد فریب است.</li> <li>- سرعت پایین‌تر نسبت به روش‌های نوری</li> </ul>
تصویربرداری	<ul style="list-style-type: none"> <li>- کلیه طیف‌های بصری و مادون قرمز را پوشش می‌دهد. (۳۰۰ گیگاهرتز تا ۳ مگاهرتز)</li> <li>- دوربین‌های IR می‌توانند در کلیه شرایط آب و هوایی و شب و روز کار کنند.</li> <li>- می‌توان از فناوری‌های رایانه‌ای نیز کمک گرفت.</li> <li>- امکان تشخیص جهت و سرعت</li> <li>- قابلیت شناسایی محموله پهبادهای را دارند.</li> <li>- می‌توانند عکس تهیه کنند و برای تحقیقات بعدی از آنها استفاده شود.</li> </ul>	<ul style="list-style-type: none"> <li>- تصاویر دو بعدی فراهم می‌کنند.</li> <li>- محدودیت عملکرد در شرایط خاص دمایی و آب و هوایی برای دوربین EO</li> <li>- وابستگی به داده‌های زمین مرجع</li> <li>- وابستگی به خط دید</li> <li>- به تنهایی قابلیت استفاده ندارند.</li> <li>- خطای نسبتاً بالایی دارند.</li> </ul>
رادار	<ul style="list-style-type: none"> <li>- محدوده باند مورد استفاده: ۳۰۰ گیگاهرتز تا ۳ مگاهرتز</li> <li>- کارکرد در کلیه شرایط آب و هوایی و دمایی و شب و روز</li> <li>- سنجش اطلاعات مربوط به سرعت هدف</li> <li>- امکان شناسایی علائم ریز</li> <li>- سطح پوشش بالا</li> <li>- دقت بالا</li> <li>- حجم محدود و قابل حمل که آن را برای کاربردهای تاکتیکی قابل استفاده می‌کند.</li> <li>- قابلیت اعتماد و اتکاء بالا</li> <li>- برد بالا</li> <li>- رصد دائمی</li> <li>- تعیین موقعیت دقیق</li> <li>- هم‌زمان توانایی شناسایی صدها هدف را دارد</li> <li>- توان شناسایی انواع مختلف پهبادهای اعم از خودکار و غیرخودکار را دارد.</li> </ul>	<ul style="list-style-type: none"> <li>- نیاز به سطح مقطع راداری بالا</li> <li>- تشخیص تفاوت پهبادهای پرنده‌ها به سختی</li> <li>- محدودیت عملکرد در ارتفاع‌ها و سرعت‌های پایین.</li> <li>- در برخورد با اشیاء کوچک بخصوص پرنده‌گان دچار اختلالاتی می‌شود.</li> <li>- وابستگی به خط دید</li> <li>- هزینه بالا</li> <li>- به کارگیری از آن نیازمند مجوز بوده و باید کنترل فرکانسی برای جلوگیری از تداخلات صورت پذیرد.</li> </ul>
تحلیل گر امواج راداری (RF)	<ul style="list-style-type: none"> <li>- گرفتن طیف‌های ارتباطی و سیگنال‌های میان پهباد و اپراتور آن</li> <li>- پیچیدگی پایین و سادگی در اجرا یا پیاده‌سازی</li> <li>- کارکرد در کلیه شرایط آب و هوایی و دمایی و شب و روز</li> <li>- سادگی نصب به خاطر مدولار بودن و دریافت سیگنال‌های دیجیتال</li> <li>- امکان در اختیار گرفتن کنترل خلبان</li> <li>- قیمت نسبتاً پایین</li> <li>- توانایی شناسایی هم‌زمان چند پهباد</li> <li>- به صورت غیرفعال (پسیو) عمل می‌کنند.</li> </ul>	<ul style="list-style-type: none"> <li>- نیاز به دانش مربوط به ارتباطات پهبادی</li> <li>- تشخیص دشوار زاویه رسیدن</li> <li>- عدم امکان استفاده در محیط‌های شهری به خاطر پدیده fading و مسیره‌های چندگانه</li> <li>- آسیب‌پذیر در برابر فرکانس‌های رادیویی غیرمجاز که ظرفیت دریافت کننده آن را بیش از حد اشغال می‌کند.</li> <li>- تأثیر منفی بر نیروهای خودی</li> <li>- قابلیت آشکارسازی و انهدام با موشک‌ها و پهبادهای ضدتشنع</li> <li>- عدم امکان شناسایی پهبادهای خودکار</li> <li>- عدم شناسایی همیشه محل دقیق پهبادهای</li> <li>- برای محدوده‌های ارتفاعی پایین کاربرد دارد.</li> </ul>

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهنادی با استفاده از روش تحلیل سلسله‌مراتبی

جدول ۲- ویژگی‌ها و محدودیت‌های روش‌های مقابله با پهنادها (چپیر و همکاران، ۲۰۲۲)، (همینگا و همکاران، ۲۰۲۲)، (پدرام مزلقانی و همکاران، ۱۳۹۵) (تجمیع و گردآوری شده توسط نگارندگان، ۱۴۰۲)

محدودیت‌ها	ویژگی‌ها	روش
<ul style="list-style-type: none"> <li>- ضروری بودن جهت‌گیری دقیق برای جمینگ</li> <li>- دشوار بودن شناسایی میزان اثرگذاری جمینگ</li> <li>- هزینه بالا</li> <li>- ریسک اختلالات غیرعمدی بسیار بالاست و امکان تخریب تجهیزات الکترونیکی پیرامونی است.</li> <li>- پهناد خاموش می‌شود و ممکن است در جایی خارج از کنترل نیروهای خودی فرود آید.</li> </ul>	<ul style="list-style-type: none"> <li>- می‌تواند مدارها و تجهیزات داخلی پهنادها را بسوزاند.</li> <li>- در دامنه‌های کوتاه و بلند قابلیت استفاده دارد.</li> </ul>	پالس‌های الکترومغناطیسی (EMP)
<ul style="list-style-type: none"> <li>- حساس به شرایط آب و هوایی</li> <li>- نیاز به اطلاعات دقیق از موقعیت هدف</li> <li>- لیزر با قدرت بالا امکان تداخل با سایر سیستم‌ها را دارد.</li> <li>- هزینه بالا</li> <li>- فناوری بالای لیزر پرتوان</li> <li>- شناسایی آسان توسط دشمن (به دلیل خط آتش مستقیم)</li> </ul>	<ul style="list-style-type: none"> <li>- در قدرت‌های پایین می‌تواند دوربین پهناد را از کار بیندازد و در قدرت‌های بالا به‌طور کلی پهناد را از کار بیندازد.</li> <li>- به راحتی می‌توان هدف را دنبال کرد.</li> <li>- امن‌تر از روش‌های فیزیکی حذف یا به‌کارگیری از پرتابه‌هاست.</li> <li>- امکان رهگیری اهداف متعدد</li> <li>- زمان عکس‌العمل پایین</li> <li>- دقت و برد بالا</li> </ul>	لیزر
<ul style="list-style-type: none"> <li>- کوچک بودن حوزه مورد حفاظت</li> <li>- امکان ایجاد تداخل با سایر سیستم‌ها</li> <li>- ناکارآمدی در برابر پهنادهای خودکار</li> <li>- ناکارآمدی در برابر پهنادهایی که سامانه ناوبری داخلی دارند.</li> <li>- ناکارآمدی در برابر پهنادهایی که سامانه ارتباطی رمزنگاری شده دارند.</li> <li>- جوابگویی صرفاً در فواصل کوتاه</li> <li>- امکان ایجاد تداخل با سایر تجهیزات</li> <li>- برد کم</li> <li>- امکان پدید آمدن رفتارهای غیرقابل پیش‌بینی برای پهناد وجود دارد.</li> <li>- امکان برخورد پهناد به هدف مورد نظر به شکل غیرعامدانه‌ای وجود دارد.</li> </ul>	<ul style="list-style-type: none"> <li>- مقرون‌به‌صرفه</li> <li>- پاسخگویی در برابر تهدیدات جمعی پهنادها</li> <li>- می‌تواند حمله پهنادهای جمعی که به‌طور هم‌زمان حمله کرده‌اند را خنثی کنند و سیگنال‌های دریافتی آنها را کاهش دهند.</li> <li>- امکان جهت‌دهی و اعمال جمینگ به‌صورت مستقیم در جهت‌های دلخواه</li> </ul>	ایجاد میدان مغناطیسی
<ul style="list-style-type: none"> <li>- نیاز به داشتن تحلیل‌های ثابت و دقیق از فرکانس‌های عملیاتی پهناد هدف</li> <li>- نیاز به سیستم سنجش طیف‌های مختلف</li> <li>- برد کم</li> <li>- امکان اثرگذاری بر سایر سامانه‌های ارتباطی</li> </ul>	<ul style="list-style-type: none"> <li>- امکان کپی و بازتولید سیگنال‌های ارتباطی با استفاده از الگوریتم‌های هوش مصنوعی و پردازش سیگنال‌های دیجیتال</li> <li>- امکان کشف آسیب‌پذیری‌های سیستم‌های مختلف</li> </ul>	جرم با فرکانس رادیویی RF/GNSS (Spoofing)

## ۲- روش تحقیق

مطالعات مروری اسناد مرتبط، داده‌ها و اطلاعات مورد نیاز گردآوری شده است. سپس بر اساس یافته‌ها و تحلیل‌های محقق از یافته‌های تحقیقاتی و کسب نظر از جامعه خبرگان

در این پژوهش که در زمره پژوهش‌های کاربردی می‌باشد و با روش تحلیلی توصیفی به انجام رسیده است، بر اساس

۵. امکان شناسایی پهنادهای خودکار (از پیش برنامه‌ریزی شده)
  ۶. محدوده یا برد عملکرد
  ۷. عملکرد در شرایط مختلف آب و هوایی و روشنایی
  ۸. دقت عملکرد
  ۹. شدت اثر بر هدف
  ۱۰. امکان فرونشاندن پهناد
  ۱۱. قابلیت بومی‌سازی در کشور در زمان کوتاه
  ۱۲. دسترسی به اطلاعات آشکار و پنهان سامانه
- پژوهش، مؤلفه‌های ارزیابی و اولویت‌بندی راهکارها تعیین گردید. در مرحله بعد با بهره‌گیری از تکنیک تحلیل سلسله‌مراتبی (AHP)، این معیارها با کسب نظر مجدد از جامعه خبرگان پژوهش و با بهره‌گیری از نرم‌افزار Expert Choice 11 رتبه‌بندی گردید. در مرحله بعد با اختصاص امتیاز به هریک از راهکارهای شناسایی و مقابله با تهدیدات پهنادی بر اساس مؤلفه‌های تعیین شده و تشکیل رابطه میانگین وزنی برای هریک از راهکارها، امتیاز نهایی هریک از راهکارها تعیین و امکان اولویت‌بندی فراهم می‌گردد.

### ۳-۱- روش AHP

فرایند تحلیل سلسله‌مراتبی (AHP)، روش تصمیم‌گیری چند معیاره‌ای است که توسط پروفیسور ساعتی در دهه ۱۹۷۰ میلادی معرفی گردید (زبردست، ۱۳۸۰). این روش به دلیل ویژگی‌های ریاضی مطلوبی که دارد و این موضوع که اطلاعات ورودی به این روش به راحتی به دست می‌آید مورد توجه بسیاری از محققان است. این روش از ساختاری چند سطحی و سلسله‌مراتبی از اهداف، معیارها، زیرمعیارها و گزینه‌ها استفاده می‌کند و اطلاعات از مقایسه‌های زوجی به دست می‌آیند (کوسالیا (Kousalya)، ۲۰۱۲).

### ۳-۲- تشکیل مقایسات زوجی

هنگامی که سلسله‌مراتب تشکیل گردید، گام بعدی آن است که اولویت‌های هریک از اجزاء سطوح تعیین گردند. مجموعه‌ای از ماتریس‌های مقایسه‌ای کلیه اجزاء در یک سطح، به ترتیب از بالاترین اولویت‌ها ساخته می‌شود. مقایسات بر این اساس شکل می‌گیرد که به‌عنوان نمونه، المان «الف» چه مقدار اهمیت بیشتری نسبت به المان «ب» دارد.

تقدم اهمیت بر اساس جدولی ۹ مقیاسی در جدول ۳ نشان داده شده است.

شایان ذکر است فرایند اختصاص امتیاز به راهکارهای شناسایی و مقابله با تهدیدات پهنادی در بازه‌ای سه‌گانه (کم: ۱، متوسط: ۲ و زیاد: ۳) و بر اساس اطلاعات موجود در منابع تحقیق صورت پذیرفته است. با این تفاسیر رویکرد این تحقیق، آمیخته (کمی-کیفی) بوده است. با توجه به تخصصی بودن موضوع پژوهش و محدودیت افراد خبره در این زمینه، خبرگان پژوهش به روش نمونه‌گیری هدفمند به تعداد ۱۰ نفر انتخاب شده‌اند.

### ۳- مؤلفه‌های مؤثر در اولویت‌بندی روش‌های شناسایی و مقابله با تهدیدات پهنادی

با مطالعه و تحلیل اسناد یاد شده در بخش ادبیات پژوهش و همچنین سایر اسنادی که مرتبط با موضوع بوده‌اند و همچنین کسب نظر از خبرگان پژوهش، تعداد ۱۲ مؤلفه به‌عنوان مؤلفه‌های برترساز در انتخاب روش‌های شناسایی و مقابله با تهدیدات پهنادی شناسایی شدند که به شرح زیر می‌باشند:

۱. سرعت واکنش سامانه
۲. هزینه به‌کارگیری سامانه
۳. اثرات جانبی بر تجهیزات و افراد
۴. مهارت لازم جهت به‌کارگیری

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهنای با استفاده از روش تحلیل سلسله‌مراتبی

### جدول ۳- مقیاس نه تایی شدت اهمیت و توضیحات مربوطه

میزان اهمیت	تعریف
۱	اهمیت برابر
۳	اهمیت نسبتاً بیشتر
۵	اهمیت با شدت بیشتر
۷	اهمیت با شدت خیلی بیشتر
۹	اهمیت فوق‌العاده بیشتر
۸، ۶، ۴، ۲	مقادیر متوسط

مبنای مقایسه دودویی معیارها یا گزینه‌ها و بر اساس مقیاس ۹ کمیته‌ی ساعتی صورت پذیرفته و نتیجه در ماتریس مقایسه دودویی معیارها یا گزینه‌ها ثبت شده و از طریق نرم‌الیزه کردن میانگین هندسی ردیف‌های این ماتریس‌ها، ضرایب اهمیت مورد نظر به دست می‌آید. در مقاله حاضر از نرم‌افزار *Expert Choice 11* برای تحلیل ماتریس‌ها استفاده می‌گردد.

اولین گام در اولویت‌بندی روش‌های مقابله با تهدیدات پهنای رتبه‌بندی مؤلفه‌های بالا بوده که با روش تحلیل سلسله‌مراتبی این اقدام صورت می‌پذیرد.

فرایند به دست آوردن وزن (ضریب اهمیت) گزینه‌ها نسبت به هریک از زیرمعیارها شبیه تعیین ضریب اهمیت معیارها نسبت به هدف است. در هر دو حالت، قضاوت‌ها بر

### جدول ۴- جدول خام تحلیل سلسله‌مراتبی

سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	شدت اثر بر هدف	امکان فرونشاندن پهناد	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
سرعت واکنش										
هزینه										
اثرات جانبی										
نیاز به مهارت										
محدوده یا برد عملکرد										
عملکرد در شرایط مختلف آب و هوایی										
دقت عملکرد										
شدت اثر بر هدف										
امکان فرونشاندن پهناد										
قابلیت بومی‌سازی در کشور در زمان کوتاه										
دسترسی به اطلاعات آشکار و پنهان سامانه										

#### ۴- ویژگی‌های جامعه خبرگان

با توجه به تخصصی بودن موضوع روش‌های شناسایی و مقابله با تهدیدات پهبادی از افراد مطلع و صاحب‌نظر در این زمینه کسب نظر گردید. لذا همان‌طور که پیش‌تر نیز اشاره شد روش انتخاب جامعه خبرگان، روش نمونه‌گیری هدفمند قضاوتی بوده است. ویژگی‌های جامعه خبرگان پژوهش به شکل زیر است:

- تعداد: ۱۰ نفر
- جنسیت: ۱۰ نفر مرد- صفر نفر زن
- مدرک تحصیلی: ۷ نفر دکتری- ۳ نفر کارشناسی ارشد
- تخصص: ۵ نفر حوزه دفاع الکترونیک - ۳ نفر حوزه حفاظت از زیرساخت‌های حیاتی- ۲ نفر حوزه دفاع سایبری

نتیجه تحلیل سلسله‌مراتبی صورت گرفته با استفاده از نرم‌افزار *Expert Choice 11* به‌قرار زیر است:

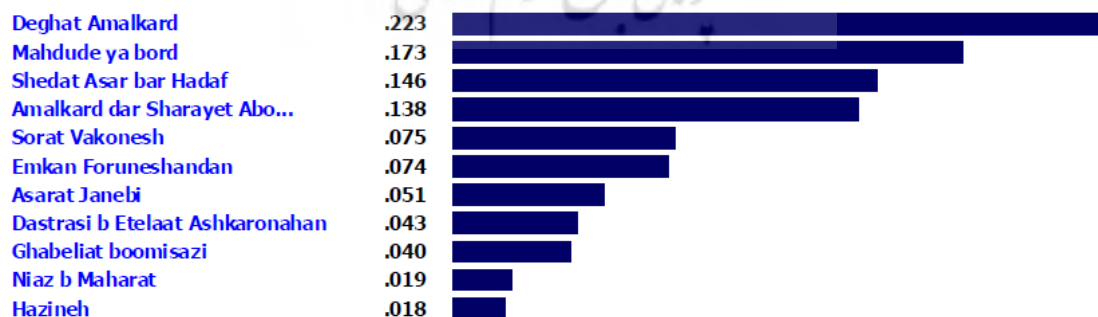
در این تحلیل ضریب ناسازگاری ۰/۰۹ بوده و از آنجا که کمتر از ۰/۱ می‌باشد مورد تأیید می‌باشد؛ بنابراین اولویت‌بندی معیارهای تعیین شده به‌صورت زیر است:

بر این اساس، دقت عملکرد سامانه با اختلاف معناداری بالاترین درجه اهمیت را نسبت به سایر معیارها دارد. بدین معنا که سامانه باید کمترین خطا را داشته و به شکل دقیقی ویژگی‌های پهباد مهاجم را شناسایی نماید. پس از آن، معیار

محدوده یا برد عملکردی سامانه می‌باشد که هر اندازه بیشتر باشد بهتر است. شدت اثرگذاری سامانه مقابله با هدف نیز حائز سومین رتبه اهمیت می‌باشد. دو معیار هزینه و نیاز به مهارت نیز به‌ترتیب حائز کمترین امتیازها می‌باشند. تفسیر این موضوع آن است که برای تأمین امنیت یک زیرساخت حیاتی در برابر تهدیدات پهبادی موضوع هزینه در برابر آنچه به دست می‌آید موضوع کم‌اهمیتی است. نیاز به مهارت کاربران نیز موضوعی نیست که به خاطر آن نوع سامانه شناسایی و مقابله نیاز به تغییر داشته باشد.

#### جدول ۵- رتبه‌بندی معیارهای رتبه‌بندی روش‌های شناسایی و مقابله با تهدیدات پهبادی

رتبه‌بندی	رتبه‌بندی	امتیاز
۱	دقت عملکرد	۰/۲۲۳
۲	محدوده یا برد عملکرد	۰/۱۷۳
۳	شدت اثر بر هدف	۰/۱۴۶
۴	عملکرد در شرایط مختلف آب و هوایی و روشنایی	۰/۱۳۸
۵	سرعت واکنش	۰/۰۷۵
۶	امکان فرونشاندن پهباد	۰/۰۷۴
۷	اثرات جانبی	۰/۰۵۱
۸	دسترسی به اطلاعات آشکار و پنهان سامانه	۰/۰۴۳
۹	قابلیت بومی‌سازی در کشور در زمان کوتاه	۰/۰۴
۱۰	نیاز به مهارت	۰/۰۱۹
۱۱	هزینه	۰/۰۱۸



Inconsistency = 0.09  
with 0 missing judgments.

نمودار ۱- نمودار میله‌ای رتبه‌بندی معیارهای رتبه‌بندی

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهنای با استفاده از روش تحلیل سلسله‌مراتبی

هریک از روش‌های شناسایی تهدیدات پهنای امتیازی از ۱ تا ۳ اختصاص داده می‌شود. به‌نحوی که ۳ مناسب‌ترین وضعیت و ۱ نامناسب‌ترین وضعیت می‌باشد.

#### ۲-۵- محاسبه امتیازات

#### ۵-۲-۱- روش‌های شناسایی

$$= \text{اکوستیک} \\ 3*0.075+3*0.018+3*0.051+3*0.019+1*0.173+1*0.13 \\ 8+1*0.223+3*0.04+3*0.043=1.27 \\ = \text{تصویربرداری} \\ 3*0.075+2*0.018+3*0.051+3*0.019+2*0.173+3*0.13 \\ 8+2*0.223+3*0.04+3*0.043=1.93$$

در مرحله بعد، هر یک از سامانه‌های معرفی شده در بخش اول پژوهش بر اساس معیارهای یاد شده امتیازدهی شده و امتیاز کلی هر روش بر اساس حاصل ضرب ضرب اهمیت معیار در امتیاز اختصاص داده شده به آن معیار برای هر یک از روش‌ها محاسبه می‌گردد.

#### ۵- تجزیه و تحلیل یافته‌ها

#### ۵-۱- امتیازدهی به روش‌های شناسایی تهدیدات

#### پهنای

در این بخش بر اساس یافته‌های حاصل از ادبیات پژوهش به

جدول ۶- امتیازات اتخاذ داده شده به هر یک از روش‌های شناسایی پهنای

سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
۲	۲	۲	۲	۱	۱	۱	۲	۲
۲	۲	۳	۳	۲	۲	۲	۲	۲
۲	۱	3	۱	۲	۲	۲	۲	۲
۲	۱	۲	۱	۲	۲	۱	۲	۲

جدول ۷- امتیازات اتخاذ داده شده به هر یک از روش‌های مقابله با پهنای

سرعت واکنش	هزینه	اثرات جانبی	نیاز به مهارت	محدوده یا برد عملکرد	عملکرد در شرایط مختلف آب و هوایی	دقت عملکرد	شدت اثر بر هدف	امکان فرونشاندن پهنای	قابلیت بومی‌سازی در کشور در زمان کوتاه	دسترسی به اطلاعات آشکار و پنهان سامانه
۲	۱	۱	۱	۲	۲	۲	۲	۲	۲	۲
۳	۱	۱	۱	۲	۱	۳	۳	۱	۲	۲
۱	۳	۱	۳	۱	۳	۲	۲	۲	۲	۱
۲	۱	۱	۱	۲	۲	۱	۲	۲	۲	۱
۲	۲	۱	۱	۲	۲	۳	۲	۲	۲	۲



قرار دارند و روش آکوستیک یا سنجنده‌های صوتی حائز پایین‌ترین امتیاز می‌باشد که عمده علت آن دقت و برد عملکردی پایین می‌باشد.

### ۵-۲-۲- روش‌های مقابله

پالس‌های الکترومغناطیسی  
 $= 2 * 0.075 + 1 * 0.018 + 1 * 0.051 + 1 * 0.019 + 3 * 0.127 + 3 * 0.138 + 38 * 2 * 0.223 + 3 * 0.146 + 2 * 0.074 + 3 * 0.04 + 2 * 0.043 = 2.41$

لیزر =  
 $3 * 0.075 + 1 * 0.018 + 1 * 0.051 + 1 * 0.019 + 3 * 0.127 + 1 * 0.138 + 3 * 0.223 + 3 * 0.146 + 1 * 0.074 + 2 * 0.04 + 2 * 0.043 = 2.32$

= ایجاد میدان الکترومغناطیسی  
 $1 * 0.075 + 3 * 0.018 + 1 * 0.051 + 3 * 0.019 + 1 * 0.127 + 3 * 0.138 + 8 + 2 * 0.223 + 3 * 0.146 + 2 * 0.074 + 2 * 0.04 + 1 * 0.043 = 1.98$

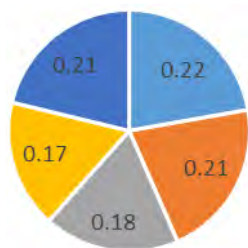
= جمینگ  
 $2 * 0.075 + 1 * 0.018 + 1 * 0.051 + 1 * 0.019 + 2 * 0.127 + 3 * 0.138 + 1 * 0.223 + 2 * 0.146 + 3 * 0.074 + 3 * 0.04 + 1 * 0.043 = 1.9$

= اسپوفینگ  
 $2 * 0.075 + 2 * 0.018 + 1 * 0.051 + 1 * 0.019 + 2 * 0.127 + 2 * 0.138 + 3 * 0.223 + 2 * 0.146 + 3 * 0.074 + 3 * 0.04 + 3 * 0.043 = 2.31$

### جدول ۹- امتیازات نرمال شده روش‌های مقابله با پهنای

نام روش	امتیاز خام	امتیاز نرمال شده
پالس‌های الکترومغناطیسی	۲,۴۱	۰,۲۲
لیزر	۲,۳۲	۰,۲۱
ایجاد میدان مغناطیسی	۱,۹۸	۰,۱۸
جمینگ	۱,۹	۰,۱۷
اسپوفینگ	۲,۳۱	۰,۲۱
مجموع	۱۰,۹۱	۱

اسپوفینگ ■ جمینگ ■ ایجاد میدان مغناطیسی ■ لیزر ■ پالس‌های الکترومغناطیسی



نمودار ۳- امتیاز نرمال شده روش‌های مقابله

رادار  
 $= 3 * 0.075 + 1 * 0.018 + 3 * 0.051 + 3 * 0.019 + 3 * 0.127 + 3 * 0.138 + 3 * 0.223 + 3 * 0.04 + 3 * 0.043 = 2.27$

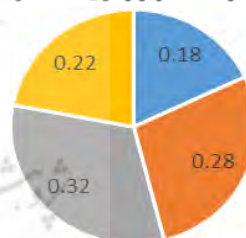
RF  
 $= 2 * 0.075 + 1 * 0.018 + 2 * 0.051 + 1 * 0.019 + 2 * 0.127 + 3 * 0.138 + 1 * 0.223 + 3 * 0.04 + 3 * 0.043 = 1.52$

در این مرحله به منظور نرمال سازی اعداد به دست آمده، جمع جبری کلیه امتیازات محاسبه شده و امتیاز هر روش تقسیم بر جمع جبری به دست آمده شده تا امتیاز نرمال شده هر روش به دست آید. جمع جبری امتیازات نرمال شده باید عدد ۱ باشد.

### جدول ۸- امتیازات نرمال شده روش‌های شناسایی پهنای

نام روش	امتیاز خام	امتیاز نرمال شده
آکوستیک	۱,۲۷	۰,۱۸
تصویربرداری	۱,۹۳	۰,۲۸
رادار	۲,۲۷	۰,۳۲
RF	۱,۵۲	۰,۲۲
مجموع	۶,۹۹	۱

رادار ■ RF ■ تصویربرداری ■ آکوستیک



نمودار ۲- امتیاز نرمال شده روش‌های شناسایی

نتایج حاصل از این جدول بیانگر آن است که روش‌های شناسایی مبتنی بر رادار، بهترین روش برای شناسایی پهنای می‌باشد؛ زیرا این روش علاوه بر آنکه توانایی شناسایی پهنای خودکار را دارد، دقت عملکردی بالایی نیز داشته و در کشور امکان ساخت آن وجود دارد. نکته قابل تأمل آن است که پهنای کوچک یا ریزپهندها با رادارهای اختصاصی و سه بعدی باید شناسایی شوند. پس از آن روش‌های تصویربرداری اپتیکال و حرارتی در رتبه بعدی

راهکارهای اولویت‌بندی شده پدافند الکترونیک و پدافند سایبری در شناسایی و مقابله با تهدیدات پهبادی با استفاده از روش تحلیل سلسله‌مراتبی

و مقابله با تهدیدات پهبادی پیش روی تصمیم‌سازان و تصمیم‌گیران این حوزه در زیرساخت‌های مختلف وجود دارد، دقت عملکردی این سامانه‌ها، محدوده یا برد عملکردی آنها و همچنین شدت اثرگذاری بر هدف، حائز بیشترین اهمیت و هزینه سامانه حائز کمترین اهمیت می‌باشند. سپس هریک از روش‌های شناسایی و مقابله در جداولی مجزا امتیازدهی شدند. از حاصل ضرب امتیازهای به‌دست‌آمده در وزن معیارها، امتیاز نهایی هر روش اکتساب گردید. بر این اساس از میان روش‌های متعدد شناسایی و مقابله با تهدیدات پهبادی در حوزه پدافند الکترونیک و پدافند سایبری، در حوزه شناسایی بهره‌گیری از سامانه‌های راداری بهترین روش برآورد گردید. همچنین روش سنجنده‌های صوتی یا آکوستیک نیز پایین‌ترین امتیاز را کسب نمود.

در حوزه مقابله نیز بهره‌گیری از پالس الکترومغناطیسی بهترین روش مقابله با تهدیدات پهبادی تشخیص داده شد. روش جمنینگ نیز هرچند روشی مرسوم و قدیمی در این حوزه محسوب می‌شود اما از آنجا که کارایی چندانی در برابر پهبادهای خودکار ندارد، حائز کمترین امتیاز می‌باشد. نتیجه عملیاتی محقق از این پژوهش آن است که باید از سامانه‌های شناسایی و مقابله ترکیبی استفاده نمود؛ یعنی سامانه حاوی حداقل دو روش برای شناسایی و دو روش برای مقابله با تهدیدات پهبادی باشد.

نتایج حاصل از ارزیابی جدول روش‌های مقابله با تهدیدات پهبادی حاکی از آن است که بهره‌گیری از پالس‌های الکترومغناطیسی (EMP) بهترین روش مقابله با تهدیدات پهبادی می‌باشد؛ زیرا این روش علاوه بر آنکه برای مقابله با پهبادهای خودکار و غیرخودکار مناسب است، امکان انجام حملات فوجی یا سوارمینگ (Swarming) را از دشمن گرفته و امنیت خوبی را برای زیرساخت فراهم می‌آورد. روش جمنینگ از آنجا که صرفاً برای مقابله با پهبادهای غیرخودکار طراحی شده، حائز کمترین امتیاز بوده و روش ایجاد میدان الکترومغناطیسی نیز محدوده اثر بسیار کم و سطح اثرگذاری غیرروشنی را دارد.

## ۶- نتیجه‌گیری

پژوهش حاضر با هدف شناسایی و اولویت‌بندی روش‌های شناسایی و مقابله با تهدیدات پهبادی به انجام رسید. در نتیجه انجام بخش مروری این پژوهش، شناخته‌شده‌ترین روش‌های شناسایی و مقابله با تهدیدات پهبادی از معتبرترین منابع معرفی و مزایا و معایب هریک از آنها بیان گردید. در ادامه طی یک فرایند تحلیل محتوا، ۱۱ معیار برای رتبه‌بندی روش‌ها تدوین و با بهره‌گیری از روش تحلیل سلسله‌مراتبی رتبه‌بندی گردیدند. در نتیجه این تحلیل مشخص گردید از میان معیارهای متفاوتی که برای انتخاب سامانه‌های شناسایی

## ۷- مراجع

- پدرام، عبدالرحیم؛ احمدیان، مهدی؛ امیرمزلقانی، یوسف (۱۳۹۷). آینده پژوهی در حوزه محصولات ضد پهپاد با استفاده از اولویت‌گذاری پابرجا / آینده پژوهی دفاعی، شماره ۱۱، ۱۴۳-۱۶۴
- حبیبی، نیک‌بخش (۱۳۹۳). پهپاد در عملیات هوایی. تهران: انتشارات راهبردی نهجا.
- خرم‌فعال، حسین (۱۳۹۹). تهدیدات ریزپرنده‌ها و راه‌های مقابله با آن. معاونت آموزش و پژوهش ستاد کل نیروهای مسلح
- رستمی، محمد (۱۳۹۱). آشنایی با هواپیماهای بدون سرنشین (پهپاد). تهران: انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- زبردست، ا. (۱۳۸۰). کاربرد فرایند تحلیل سلسله‌مراتبی در برنامه‌ریزی شهری و منطقه‌ای، نشریه هنرهای زیبا، شماره ۱۰، تهران.
- شکوهی، حسین (۱۳۹۲). نقش پهپادها در جنگ‌های آینده (صحنه نبرد ناهمگون). تهران: دانشگاه عالی دفاع ملی.
- فرحبخت، احمدرضا؛ دهقانی، مهدی (۱۳۹۸). همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی. فصلنامه امنیت ملی، شماره ۳۱، ۱۹۹-۲۱۹.
- کافی، سعید (۱۴۰۰). درس آموخته‌های جنگ قره‌باغ. تهران: دانشگاه جامع امام حسین علیه‌السلام.
- کاظمی، حمید؛ و الهیان، سمانه (۱۳۹۹). توسعه پهپادهای غیرنظامی و چالش‌های پیش روی آن. فصلنامه فناوری در مهندسی هوافضا، ۴۵-۶۴.
- نوروزی، احمد (۱۳۹۴). بررسی حملات الکترونیکی علیه پهپادها. چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه. تهران.
- Brust, M., Danoy, G., Bouvry, P., Gashi, D., Pathak, H., & Goncalves, M. (2018). Defending against Intrusion of Malicious UAVs with Networked UAV Defense Swarms.
- Chiper, F.-L., Martian, A., Vladeanu, C., Marghescu, I., Craciunescu, R., & Fratu, O. (2022). Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution. *Sensors*.
- Farlik, J., Kratky, M., Casar, J., & Stary, V. (2019). Multispectral Detection of Commercial Unmanned Aerial Vehicles. *Sensors*.
- Hamminga, S., Claasen, T. & Verdonk, M. (2022). *Counter-Drone Technologies to Detect and Stop Drones Today*. Retrieved from: <https://www.robinradar.com/>
- Holland, M.A. (2018). Counter-Drone Systems. Center for the Study of the Drone at Bard College, Feburary <http://dronecenter.bard.edu/counter-drone-systems/>
- Kratky, M., & Farlik, J. (2018). Countering UAVs – the Mover of Research in Military Technology. *Defence Science Journal*, 460-466.
- Kousalya, P. (2012). Analytical Hierarchy Process approach – An application. *Mathematica Aeterna*, 2(10), 861-878.