Defensive Researches and Management

Optimal Model of Multi-Layered Air Defense of the Islamic Republic of Iran: A Strategic Shift from System-Centric to Network-Centric Integration in Response to Modern Air-Based Threats

Yaser Khorrami [1] * | Seyed Mohammad Javad Navandi shiraz [2]

1. Corresponding Author: Assistant Professor, Department of Electrical and Electronics Engineering, Imam Hossein Comprehensive University, Tehran, Iran. Email: y.khorrami@ihu.ac.ir

2. Master's student, Islamic Studies and Political Science, Imam Sadiq University, Tehran, Iran.

Volume info

Vol. 25
Series: 112
Spring 2026
P.P: 11-30

Article Type

Research Paper

Article History

Received:
2025-12-23
Revised:
2026-02-27
Accepted:
2026-09-05
Published:
2026-09-05

ISSN – E-ISSN

ISSN: 2008-6121
E-ISSN: 2645-5218

Abstract

Rapid changes in the nature of air-based threats, especially the emergence of combined salvo attacks including ballistic and cruise missiles, mass drones, and electronic warfare, have seriously challenged the classic air defense structures. Due to its geopolitical location and continuous threats, the Islamic Republic of Iran is increasingly exposed to these types of complex threats. The present study, with an analytical-descriptive approach and comparative studies, while analyzing the nature of new threats, explains the necessity of transitioning from a system-oriented model to a multilayered and network-oriented air defense model. The proposed framework is based on three fundamental principles: structural resilience through a decentralized cluster architecture, a smart defense economy based on the combination of capabilities, and cognitive superiority using data-centricity and light artificial intelligence. This model shows that by redefining the criteria for success from absolute impenetrability to increasing the cost to the attacker, sustainable, cost-effective, and repeatable air security can be created. On the eve of a conceptual revolution in defense thinking, this article outlines the transition path from technological superiority to intelligent resilience and emphasizes the need for interdisciplinary collaboration and rethinking long-held assumptions in security studies.

Keywords: Resilient air defense, new airborne threats, salvo attacks, multilayer network-based model.

Cite this Article: Khorrami, Y., Navandi shiraz, S.M.J (2026). Optimal Model of Multi-Layered Air Defense of the Islamic Republic of Iran: A Strategic Shift from System-Centric to Network-Centric Integration in Response to Modern Air-Based Threats. Scientific Journal of Defensive Researches and Management, 25(112), 11-30.
https://dor.isc.ac/dor/20.1001.1.20086121.1405.25.112.1.8

© Author(s) retain the copyright and full publishing rights

Publisher: Imam Hossein University.

الگوی مطلوب پدافند هوائی چندلایه؛ گذار راهبردی از سامانه‌محوری به یکپارچگی شبکه محور در مواجهه با تهدیدات هواپایه نوین

یاسر خرمی *[۱] | سید محمد جواد ناوندی شیراز [۲]

۱. نویسنده مسئول: استادیار، گروه برق و الکترونیک، دانشگاه جامع امام حسین(ع)، تهران، ایران.
Email: y.khorrami@ihu.ac.ir
۲. دانشجوی کارشناسی ارشد، رشته معارف اسلامی و علوم سیاسی، دانشگاه امام صادق(ع)، تهران، ایران.

چکیده

تحولات سریع در ماهیت تهدیدات هواپایه، به‌ویژه ظهور حملات سالوو ترکیبی شامل موشک‌های بالستیک و کروز، پهپادهای انبوه و جنگ الکترونیک، ساختارهای کلاسیک پدافند هوایی را با چالش جدی مواجه ساخته است. جمهوری اسلامی ایران به‌دلیل موقعیت ژئوپولیتیکی و تهدیدات مستمر، بیش از پیش در معرض این نوع تهدیدات پیچیده قرار دارد. پژوهش حاضر با رویکرد تحلیلی–توصیفی و مطالعات تطبیقی، ضمن واکاوی ماهیت تهدیدات نوین، ضرورت گذار از الگوی سامانه‌محور به مدل پدافند هوایی چندلایه و شبکه‌محور را تبیین می‌کند. چارچوب پیشنهادی بر سه اصل بنیادین استوار است: تاب‌آوری ساختاری از طریق معماری خوشه‌ای غیرمتمرکز، اقتصاد دفاعی هوشمند مبتنی بر ترکیب قابلیت‌ها و برتری شناختی با بهره‌گیری از داده‌محوری و هوش مصنوعی سبک. این مدل نشان می‌دهد که با بازتعریف معیارهای موفقیت از نفوذناپذیری مطلق به افزایش هزینه برای مهاجم، می‌توان امنیت هوایی پایدار، مقرون‌به‌صرفه و قابل تکرار ایجاد کرد. این مقاله در آستانه انقلاب مفهومی در اندیشه دفاعی، مسیر گذار از برتری فناورانه به تاب‌آوری هوشمند را ترسیم کرده و بر ضرورت همکاری بین‌رشته‌ای و بازاندیشی مفروضات دیرینه در مطالعات امنیتی تأکید می‌ورزد.

کلیدواژه‌ها: پدافند هوائی تاب‌آور، تهدیدات هواپایه نوین ، حملات سالوو، مدل شبکه‌محور چندلایه.

استناد: خرمی، یاسر و ناوندی شیراز، سیدمحمدجواد. (۱۴۰۵). الگوی مطلوب پدافند هوائی چندلایه؛ گذار راهبردی از سامانه‌محوری به یکپارچگی شبکه محور در مواجهه با تهدیدات هواپایه نوین. فصلنامه مدیریت و پژوهش های دفاعی، ۲۵(۱۱۲)، ۱۱-۳۰.
https://dor.isc.ac/dor/20.1001.1.20086121.1405.25.112.1.8

© نویسنده(گان) حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جام امام حسین(ع).

مقدمه

تهدیدات نوین هواپایه یکی از پیچیده‌ترین و بحرانی‌ترین چالش‌هایی است که در دهه‌های اخیر امنیت ملی کشورها را تهدید کرده است؛ در این میان، جمهوری اسلامی ایران به‌واسطه موقعیت ژئوپولیتیکی خود در خاورمیانه و حضور قدرت‌های نظامی بزرگ در پیرامونش، به‌طور مستمر در معرض این تهدیدات قرار دارد (حسن، ۲۰۲۱: ۴۴). این تهدیدات، که نه تنها از سوی قدرت‌های فرامنطقه‌ای چون ایالات متحده آمریکا و رژیم صهیونیستی بلکه از جانب برخی قدرت‌های منطقه‌ای نیز به‌طور فزاینده‌ای اعمال می‌شوند، به‌ویژه در قالب حملات هوایی، موشکی و جنگ الکترونیکی، ساختارهای دفاعی ایران را به شدت در معرض تهدید قرار داده‌اند. این تهدیدات با بهره‌گیری از فناوری‌های پیشرفته و تاکتیک‌های نامتقارن، مانند سرعت بالا، دقت زیاد و کمینه‌سازی نشانه‌های ردیابی[۱]، می‌توانند از سد سامانه‌های دفاعی پیشرفته عبور کنند (گرتلر، ۲۰۱۲ :۵۸). به عنوان مثال، دشمنان می‌توانند با اجرای حملات انبوه و هم‌زمان متشکل از ده‌ها یا حتی صدها موشک هدایت‌شونده و پهپاد تهاجمی، سامانه‌های پدافندی متعارف را اشباع کرده و کارایی آن‌ها را مختل نمایند.

پدافندهای هوایی متداول به‌عنوان یکی از ارکان اصلی حفظ تمامیت ارضی و امنیت هر کشور، همچنان به سامانه‌های دفاعی سامانه محور (نقطه‌ای) وابسته هستند که در برابر تهدیدات نوین از جمله پهپادها، موشک‌های کروز و حملات سایبری کارایی محدودی دارند. این سامانه‌ها اگرچه در گذشته و در مقابله با تهدیدات سنّتی هوایی موفق عمل کرده‌اند، اما در برابر تهدیدات چندوجهی و پیچیده امروزی، از جمله حملات ترکیبی و همزمان دشمن، توانایی مقابله مؤثر را ندارند. یکی از اساسی‌ترین چالش‌ها در این حوزه، ناتوانی در ایجاد یکپارچگی بین سامانه‌های پدافندی مختلف است؛ این عدم یکپارچگی موجب کاهش دقت و سرعت واکنش در برابر تهدیدات پیچیده و هماهنگ می‌شود.

---

۱ منظور از کمینه‌سازی نشانه‌های ردیابی، مجموعه اقدامات فناورانه و تاکتیکی شامل کاهش سطح مقطع راداری، کاهش آثار حرارتی، محدودیت انتشار امواج الکترومغناطیس و بهره‌گیری از پروفایل پروازی خاص است که به منظور افزایش بقاپذیری سامانه‌های هوایی در برابر ردیابی شبکه‌های پدافندی دشمن طراحی می‌شوند.

به همین دلیل، گذار از سامانه‌های دفاعی سنّتی به یک الگوی پدافند هوایی چندلایه و شبکه‌محور که بتواند به‌طور مؤثر در برابر تهدیدات نوین هواپایه واکنش نشان دهد، امری ضروری است.

در واقع، چالش دفاع در برابر این تهدیدات را می‌توان به صورت یک رقابت سالوو[1] تلقی کرد که در آن هر یک از طرف‌های درگیر قادرند با به‌کارگیری تعداد زیادی تسلیحات هدایت‌شونده، مانند انواع موشک‌ها و پهپادها، حمله کرده و در عین حال از خود دفاع کنند. در چنین رقابتی هر طرف می‌کوشد با بهبود مستمر کمّیت و بقاپذیری حملات تهاجمی خود و نیز افزایش مرگ‌باری و ظرفیت سامانه‌های دفاعی‌اش، برتری را به دست آورد (رهبرگ و گانزینگر، ۲۰۱۸ :۳).

درک ابعاد و پیچیدگی این تهدیدات و طراحی یک استراتژی دفاعی منسجم، مستلزم تحلیل دقیق تهدیدات از جنبه‌های فنی، راهبردی و ژئوپولیتیکی است؛ بر این اساس، این مقاله با تجزیه و تحلیل تهدیدات هواپایه از سوی آمریکا و رژیم صهیونیستی، به‌ویژه حملات ایالات متحده آمریکا و رژیم صهیونیستی به ایران در آبان ۱۴۰۳ و خرداد ۱۴۰۴ و بررسی نقاط ضعف سامانه‌های پدافندی امروزی، در پی معرفی و بومی‌سازی الگویی مطلوب برای پدافند هوایی چندلایه است (کانسیان، ۲۰۲۴). در این راستا، تحقیق حاضر به دنبال پاسخ به این پرسش اساسی است که چگونه می‌توان از یک سیستم پدافند هوایی سامانه‌محور و غیریکپارچه به یک مدل پدافند هوایی چندلایه و شبکه‌ای منتقل شد تا بتوان به‌طور مؤثر در برابر تهدیدات نوین ایستادگی کرد.

اهمیت این موضوع در دو سطح قابل تبیین است: نخست در سطح امنیت ملی، پدافند هوایی به‌عنوان خط مقدم دفاع هوایی از اهمیت بی‌بدیلی برخوردار است و تحلیل دقیق تهدیدات جدید و شناسایی ضعف‌های سامانه‌های دفاعی برای جلوگیری از وقوع فاجعه‌های امنیتی در صورت حملات هوایی گسترده ضرورت دارد. دوم در سطح راهبردی، بهره‌گیری از فناوری‌های نوین برای ایجاد یک سامانه پدافند هوایی یکپارچه و چندلایه می‌تواند ضمن حفظ بازدارندگی، زمینه تبدیل شدن به یک قدرت پیشرو در عرصه دفاع هوایی را فراهم سازد.

---

۱ Salvo: در پدافند هوایی به وضعیتی گفته می‌شود که دشمن تعداد زیادی موشک یا پهپاد را به‌طور همزمان شلیک می‌کند تا سامانه‌های دفاعی کشور هدف را اشباع کند. در این حالت، پدافند باید بتواند با مدیریت منابع محدود (موشک‌های رهگیر، رادارها و زمان واکنش) بیشترین تعداد تهدید را نابود کند.

در ادامه، ابتدا تهدیدات نوین، از جمله موشک‌های بالستیک، موشک‌های کروز، پهپادها و نظایر آن که تأسیسات ثابت را هدف می‌گیرند، بررسی می‌شود. سپس چالش‌های دفاعی کنونی مورد واکاوی قرار گرفته و ضرورت تغییر رویکرد پدافند تبیین می‌گردد. در گام بعد، یک مدل دفاع لایه‌ای متشکل از لایه‌های بیرونی، میانی و درونی برای پدافند هوائی معرفی شده و فناوری‌های نوینی نظیر لیزرهای انرژی‌بالا، سلاح‌های مایکروویو پرقدرت، موشک‌های هوابه‌هوای دوربرد و پهپادهای رزمی، در چارچوب این مدل تشریح می‌شود. در ادامه با ارائه شبیه‌سازی از مدل، نتایج بررسی و درنهایت تحلیل تطبیقی و ارزیابی گزینه‌ها ارائه و با جمع‌بندی و پیشنهادها به پایان خواهد رسید.

مبانی نظری

مبانی نظری این پژوهش بر سه چارچوب مفهومی اصلی و سه نظریه نوین استوار است؛ نظریه رقابت سالوو[1]، نظریه پدافند لایه‌ای[2] و رویکرد دفاع شبکه‌محور[3] مبانی نظری اصلی چارچوب تحلیلی پژوهش حاضر را به شرح ذیل تشکیل می‌دهند:

۱. نظریه رقابت سالوو[4] که توسط اندیشکده‌هایی نظیر مرکز ارزیابی‌های راهبردی و بودجه[5] توسعه یافته، بیان می‌کند که در نبردهای مدرن، برتری نظامی نه صرفاً به کیفیت سامانه‌ها، بلکه به توان تولید و مدیریت حجم حمله و دفاع وابسته است (هاگز، ۱۹۹۵). در این چارچوب، مهاجم می‌کوشد با اجرای حملات انبوه و کم‌هزینه، ظرفیت دفاعی مدافع را فرسوده و اشباع کند (بیمن، ۲۰۲۱: ۱۵)

۲. نظریه پدافند لایه‌ای بر این اصل استوار است که دفاع کارآمد مستلزم توزیع تهدید در فواصل، ارتفاعات و زمان‌های مختلف است؛ این نظریه تأکید می‌کند که اتکای صرف به یک لایه دفاعی، احتمال شکست را به‌شدت افزایش می‌دهد و تنها معماری چندلایه می‌تواند بقای تاسیسات حیاتی را تضمین نماید (والتز، ۱۹۷۹).

۳. رویکرد دفاع شبکه‌محور، هماهنگی بلادرنگ میان سنسورها، سامانه‌های رهگیر و مراکز فرماندهی و کنترل را شرط اساسی موفقیت می‌داند؛ در این رویکرد، قدرت دفاعی از سطح

1 Salvo Competition
2 Layered Air and Missile Defense
3 Network-Centric Defense
4 Salvo Competition Theory
5 CSBA

عملکرد مستقل سامانه‌ها فراتر رفته و در قالب یک شبکه هم‌افزا به عنوان دفاع داده‌محور تجلی می‌یابد (آلبرت و همکاران، ۱۹۹۹).

مبانی نوین در قالب سه نظریه زیر در مدل پیشنهادی در این مقاله استفاده شده است:

۱. نظریه سیستم‌های پیچیده تطبیق‌پذیر[1]: بیان می‌کند که سیستم‌های زنده از طریق تعامل مؤلفه‌های مستقل و خودسازمان‌دهی، قدرت تاب‌آوری ایجاد می‌کنند (میلر و پیج، ۲۰۰۷).

۲. نظریه تاب‌آوری سایبر-فیزیکی[2] : بیانگر این موضوع است که سیستم‌های مدرن باید در برابر شوک‌های همزمان در حوزه‌های فیزیکی و سایبری مقاوم باشند (لینکوف و کات، ۲۰۱۹).

۳. نظریه بهینه‌سازی چندهدفه تحت محدودیت[3]: بیان می‌کند که در شرایط محدودیت، باید چند هدف متعارض را همزمان بهینه کرد (دب، ۲۰۰۱).

پیشینهٔ پژوهش

مطالعات مربوط به پدافند هوایی در دهه‌های اخیر عمدتاً بر سه محور اصلی متمرکز بوده‌اند: ۱) تحول در تهدیدات، ۲) توسعه راهبردها و ساختارهای دفاعی و۳) فناوری‌های تحول‌آفرین.

۱. تحول در ماهیت و تاکتیک‌های تهدیدات هواپایه: مطالعات جدید بر پیچیدگی فزاینده تهدیدات در قالب «حملات ترکیبی و ازدحامی[4] و بهره‌گیری مهاجمان از هوش مصنوعی و خودمختاری» تأکید دارند. کافمن و فینک (۲۰۲۱) به تحلیل استفاده گسترده و ارزان از پهپادها در درگیری‌های اخیر و تأثیر آن بر موازنه نظامی می‌پردازد. اسچار (۲۰۱۸) نیز تحولات جنگ‌افزارهای خودمختار و پیامدهای آن برای دفاع را به صورت بنیادی بررسی می‌کند. این تهدیدات، پنجره زمانی واکنش را به شدت کاهش داده و نیاز به سیستم‌های دفاعی خودکار و مبتنی بر هوش مصنوعی را پررنگ کرده‌اند. گرتلر (۲۰۱۲) به بررسی تغییر ماهیت تهدیدات، به‌ویژه رشد موشک‌های کروز و پهپادهای ارزان‌قیمت، پرداخته و بر برتری اقتصادی مهاجم در حملات انبوه تأکید دارد (گرتلر، ۲۰۱۲: ۶۴)؛ در ادامه، رهبرگ و گانزینگر (۲۰۱۸) در چارچوب

1 Complex Adaptive Systems Theory
2 Cyber-Physical Resilience Theory
3 Multi-Objective Optimization under Constraints
4 Swarm & Hybrid Attacks

نظریه رقابت سالوو نشان می‌دهند که سامانه‌های پدافندی نقطه‌ای، حتی در صورت پیشرفت فنی، در برابر حملات ترکیبی دچار فرسایش سریع می‌شوند (رهبرگ و گانزینگر، ۲۰۱۸: ۱۲).

۲. توسعه راهبردهای دفاعی نوین: در پاسخ به تهدیدات، ادبیات راهبردی، مفاهیمی فراتر از پدافند لایه‌ای صرف را مطرح کرده‌اند. مفهوم «دفاع یکپارچه در سطوح مختلف» بر هماهنگی عمیق پدافند هوایی با سامانه‌های دفاع موشکی، جنگ الکترونیک و عملیات سایبری تأکید می‌کند. وزارت دفاع آمریکا (۲۰۲۰)، در سند راهبردی رسمی، چارچوب کنونی دفاع یکپارچه آمریکا را تشریح کرده و بر شبکه‌محوری، داده‌محوری و جنگ اطلاعات به عنوان ارکان اصلی تأکید دارد. اکتون (۲۰۲۰) نیز راهبردهای پیش‌دستانه و غیرسینتیکی مانند جنگ سایبری یا الکترونیک برای خنثی‌سازی موشک‌ها «قبل از پرتاب» را بررسی می‌کند که مکمل حیاتی دفاع سینتیک سنتی است.

۳. نقش فناوری‌های تحول‌آفرین در اثربخشی پدافند: پیشینه پژوهشی جدید، به‌طور خاص بر نقش «همگرایی فناوری‌ها» مانند هوش‌مصنوعی، کلان‌داده، محاسبات ابری و اینترنت اشیاءدر ایجاد «سامانه‌های سایبر-فیزیکی» برای دفاع هوایی تأکید می‌کند. این فناوری‌ها، هسته مرکزی تحقق دفاع شبکه‌محور و داده‌محور هستند. در این راستا، بریملی (۲۰۲۱) به تحلیل نقش هوش مصنوعی در تسریع چرخه شناسایی-تصمیم-درگیری و مدیریت نبرد در محیط‌های پیچیده می‌پردازد. کات و پرکونتی (۲۰۱۸) نیز مفهوم «اینترنت چیزهای نبرد» را مطرح می‌کنند که در آن سنسورها، سامانه‌های سلاح و سربازان در یک شبکه عظیم و هوشمند یکپارچه می‌شوند.

۴. بررسی تطبیقی و نقاط کور پژوهشی: اگرچه مطالعات تطبیقی بر روی کشورهای پیشرفته متمرکزند، تحقیقات معدودی به چالش‌های کشورهای دارای منابع محدود یا کشورهای تحت تحریم در پیاده‌سازی این سیستم‌های پیشرفته پرداخته‌اند. چالش‌هایی مانند وابستگی فناوریکی، محدودیت مالی، و نیاز به معماری‌های ترکیبی (هیبرید) که از سامانه‌های سطح بالا و پایین به‌طور همزمان استفاده می‌کنند. برای نمونه فاتر و زالا (۲۰۲۱) به راهبردهای دفاع موشکی کشورهای منطقه خاورمیانه با توجه به محدودیت‌ها و انتخاب‌های راهبردی آن‌ها می‌پردازد. حبیبی و گرار (۲۰۲۰) نیز به تحلیل توانمندی‌های تهاجمی و دفاعی یک کشور تحت تحریم و راهبرد بومی‌سازی آن می‌پردازند.

با در نظر گرفتن مبانی فوق، خلأ پژوهشی حاضر نه تنها در عدم ارائه یک مدل بومی‌شده، بلکه در عدم توجه کافی به مؤلفه‌های حیاتی عصر جدید در الگوهای بومی است. این مؤلفه‌ها شامل: چگونگی ادغام هوش مصنوعی و تحلیل داده در معماری دفاعی با منابع محدود، طراحی راهبردهای ترکیبی سینتیک و غیرسینتیک (الکترونیک/سایبر) و تطبیق اصول دفاع یکپارچه شبکه‌محور با الزامات ژئوپولیتیک و فناورانه خاص یک منطقه یا کشور می‌باشد. بنابراین، این پژوهش درصدد است تا با ترکیب چارچوب‌های نظری کلاسیک (مانند سالوو و پدافند لایه‌ای) با مفاهیم نوین (دفاع داده‌محور و هوشمند)، مدلی بومی و عملیاتی ارائه نماید که پاسخگوی تهدیدات ترکیبی و ازدحامی در شرایط دارای محدودیت باشد.

روش‌شناسی پژوهش

این پژوهش از نظر هدف، کاربردی-توسعه‌ای و از نظر ماهیت و روش، در زمره پژوهش‌های کیفی قرار می‌گیرد. هدف اصلی آن، ارائه یک مدل مفهومی بومی برای پدافند هوایی چندلایه در مواجهه با تهدیدات نوین هواپایه است. از آنجا که این تحقیق بدون دخالت مستقیم محقق در محیط عملیاتی و صرفاً از طریق مطالعه و تحلیل عمیق منابع مکتوب و گزارش‌های موجود انجام شده است، استراتژی اصلی آن تحلیل اسنادی می‌باشد.

این تحقیق با استفاده از رویکرد کیفی و استقرایی انجام شده است. استراتژی اصلی پژوهش، مطالعه اسنادی و کتابخانه‌ای عمیق همراه با تحلیل محتوای کیفی منابع مرتبط است. دلیل انتخاب این روش، ماهیت مسئله پژوهش است که نیازمند اکتشاف مفاهیم، مؤلفه‌ها و الگوهای موجود در منابع معتبر علمی و گزارش‌های میدانی جنگ‌های اخیر است. همچنین، برای شناسایی شکاف‌های موجود میان الگوهای رایج پدافندی (آمریکا، روسیه، چین، رژیم صهیونیستی) و نیازمندی‌های بومی، از روش مطالعه تطبیقی بهره گرفته شده است.

قلمرو زمانی پژوهش، عمدتاً منابع منتشرشده از سال ۲۰۱۰ تا ۲۰۲۴ را در بر می‌گیرد تا تحولات فناورانه و تاکتیکی دو دهه اخیر به‌طور کامل پوشش داده شود.

ابزار گردآوری داده‌ها در این پژوهش، فیش‌برداری هدفمند و جدول‌های استخراج داده بوده است. داده‌های گردآوری‌شده از اسناد و منابع، با استفاده از تحلیل محتوای کیفی و به کارگیری

رویکرد کدگذاری استقرایی مورد تجزیه‌وتحلیل قرار گرفتند. برای اطمینان از روایی بودن یافته‌ها، از راهبرد مثلث‌سازی منابع داده استفاده شده است. پس از استخراج مؤلفه‌ها و ارکان مدل از تحلیل متون، مدل نهایی در قالب یک نمودار مفهومی ترسیم و سپس به صورت توصیفی-تحلیلی تبیین گردید. برای اعتبارسنجی تطبیقی مدل، ارکان و مؤلفه‌های آن با الگوهای پدافندی کشورهای پیشرفته (آمریکا، روسیه، چین و رژیم صهیونیستی) مقایسه سیستماتیک شده و مزیت‌های رقابتی مدل پیشنهادی نشان داده شده است.

سؤالات پژوهش

سوال اصلی

۱- الگوی مطلوب پدافند هوایی برای مقابله مؤثر با تهدیدات نوین هواپایه چیست؟

سوالات فرعی

۱-مهم‌ترین مؤلفه‌های تهدیدات هواپایه نوین علیه تاسیسات حیاتی کدام‌اند؟

۲-چالش‌های ساختاری و فناورانه پدافند هوایی در برابر حملات سالوو چیست؟

۳-الگوی پدافند چندلایه در کشورهای پیشرفته چه ویژگی‌هایی دارد؟

۴-نقش فناوری‌های نوظهور در کاهش برتری اقتصادی مهاجم و ارتقاء پدافند هوایی چندلایه شبکه محور چیست؟

۵-الزامات بومی‌سازی یک مدل پدافند هوایی چندلایه و شبکه‌ای کدام‌اند؟

یافته‌های پژوهش

۱ .تهدیدات نوین هواپایه: تاسیسات حیاتی امروز با تهدیدات چندبُعدی مواجه‌اند که سرعت، دقت، حجم و پیچیدگی بالایی داشته و هزینه پایینی برای مهاجم دارند. این تحول، دفاع نقطه‌ای کلاسیک را در برابر حملات ترکیبی ناکارآمد ساخته است. تجارب جنگ‌های اخیر نشان می‌دهد دشمنان ایران توان بهره‌برداری از ماتریس حملات چندسکویی شامل موشک بالستیک، کروز، پهپاد و جنگ الکترونیک را برای اشباع پدافند دارند (حسن، ۲۰۲۱: ۵۲؛ رهبرگ و گانزینگر، ۲۰۱۸: ۱۲-۱۰). پنج دسته تهدید اصلی عبارت‌اند از:

- موشک‌های بالستیک مانورپذیر: نسل جدید با قابلیت تغییر مسیر در فاز پایانی و سرعت ۲۰-۵ ماخ، رهگیری را دشوار و زمان واکنش را به چندده ثانیه محدود کرده است (گرتلر، ۲۰۱۲: ۲۳).
- موشک‌های کروز کم‌ارتفاع: با بهره‌گیری از فناوری پنهانکاری و پرواز در میان موانع طبیعی، از دید رادارهای زمینی پنهان می‌مانند و خطای دایره‌ای کمتر از ۲ متر دارند (رهبرگ و گانزینگر، ۲۰۱۸: ۱۴).
- پهپادها و مهمات پرسه‌زن: قیمت پایین و امکان تولید انبوه، اقتصاد دفاع را برهم زده است؛ هزینه رهگیری هر پهپاد برای مدافع ۵۰ هزار تا یک میلیون دلار در برابر هزینه ناچیز مهاجم (گرتلر، ۲۰۱۲: ۶۴).
- حملات ترکیبی اشباع‌ساز: الگوی چهارموجی شامل: ۱) جنگ سایبری و الکترونیک، ۲) پهپاد و کروز برای اشباع، ۳) موشک بالستیک برای انهدام، ۴) مهمات دقیق‌زن برای تکمیل مأموریت (رهبرگ و گانزینگر، ۲۰۱۸: ۲۳-۲۰).
- جنگ الکترونیک: اختلال در شبکه فرماندهی و کنترل، رادارها و پیوندهای داده به‌عنوان مرحله آغازین حملات (گرتلر، ۲۰۱۲: ۴۱).

۲ . چالش‌های پدافند سنتی: ساختارهای کنونی با هفت چالش اساسی مواجه‌اند که شکاف عمیقی با نیازهای عصر رقابت سالوو ایجاد کرده است (رهبرگ و گانزینگر، ۲۰۱۸: ۲۸):

- ساختار سامانه‌محور: نبود یکپارچگی شبکه‌ای، سرعت واکنش و دقت رهگیری را کاهش می‌دهد (همان: ۲۹).
- کمبود ظرفیت مقابله با حملات انبوه: نسبت نامتوازن سالوو دفاعی به تهاجمی و هزینه بالای رهگیری (گرتلر، ۲۰۱۲: ۶۱).
- محدودیت در لایه‌بندی دفاعی: فقدان لایه بیرونی، بار دفاعی را به لایه درونی منتقل می‌کند (رهبرگ و گانزینگر، ۲۰۱۸: ۳۲-۳۳).
- ضعف در برابر تهدیدات کم‌ارتفاع: نقاط کور رادارهای زمینی و نیاز به سنسورهای هوابرد (گرتلر، ۲۰۱۲: ۵۵).
- آسیب‌پذیری در برابر جنگ الکترونیک: اختلال در هم‌زمان‌سازی داده‌ها و کاهش دقت رهگیری (همان: ۴۱).

- ناتوانی اقتصادی در برابر حملات ارزان: برتری هزینه‌ای مهاجم در حملات انبوه، ضرورت حرکت به سوی سلاح‌های کم‌هزینه مانند لیزر را ایجاب می‌کند.
- محدودیت دارایی‌های هوابرد: کمبود جنگنده‌های رهگیر، پهپادهای اطلاعاتی و سنسورهای هوابرد (رهبرگ و گانزینگر، ۲۰۱۸: ۴۷).

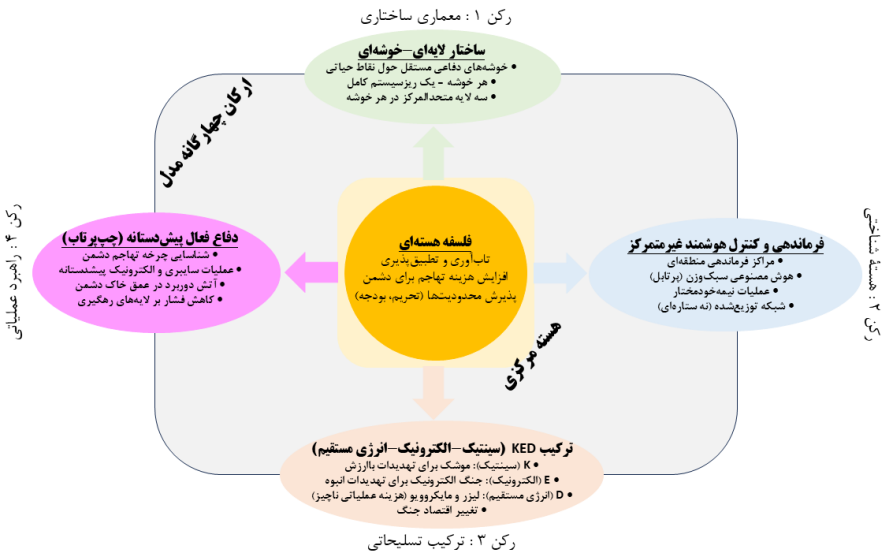
۳ .ضرورت تغییر رویکرد پدافندی: جنگ اوکراین (زابروسکی و همکاران، ۲۰۲۳) و جنگ ۱۲ روزه ایران و اسرائیل (۲۰۲۵-۲۰۲۴) آسیب‌پذیری پدافند سنتی را آشکار ساخت. در وعده صادق ۱، هزینه ۵۰-۳۰ میلیون دلاری ایران در برابر ۱.۳۵-۱.۱ میلیارد دلار دفاع اسرائیل (نسبت ۱:۳۰) نظریه شکست اقتصاد دفاع سنتی را تأیید کرد (رهبرگ و گانزینگر، ۲۰۱۸). در وعده صادق ۲، عبور موشک‌های ایران از پدافند اسرائیل و اصابت به پایگاه‌های نواتیم و تل‌نوف و متعاقباً تضعیف پدافند ایران در حملات تلافی‌جویانه)، نشان داد صرف برخورداری از سامانه‌های پیشرفته بدون «تاب‌آوری شناختی» و «معماری غیرمتمرکز» کافی نیست (موسسه بین‌المللی مطالعات راهبردی، ۲۰۲۵؛ کانسیان، ۲۰۲۴).

دفاع هوایی گذشته بر مبنای مقابله با تهاجمات محدود طراحی شده بود، اما امروز در عصر «رقابت سالوو»، بازدارندگی به توان شبکه، لایه‌بندی و سرعت واکنش بستگی دارد (رهبرگ و گانزینگر، ۲۰۱۸: ۵۳). راهکار، ایجاد معماری لایه‌ای است که در آن هر لایه بخشی از تهدید را مدیریت کند. لایه بیرونی شامل سنسورهای هوابرد (برای کشف زودهنگام تهدیدات کم‌ارتفاع)، هواگردهای رهگیر، پهپادهای اطلاعاتی-رزمی، موشک‌های هوا به هوای دوربرد و سلاح‌های انرژی‌بالا (لیزر و مایکروویو) است که با هزینه عملیاتی ناچیز، گزینه پایدار در برابر حملات انبوه محسوب می‌شوند (گرتلر، ۲۰۱۲: ۴۸، ۷۳؛ رهبرگ و گانزینگر، ۲۰۱۸: ۶۹-۶۸). لایه درونی شامل سامانه‌های پدافند نقطه‌ای (توپ‌های هوشمند و موشک‌های کوتاه‌برد) و سلاح‌های انرژی هدایت‌شده کوتاه‌برد است که آخرین خط دفاعی را تشکیل می‌دهند (گرتلر، ۲۰۱۲: ۵۸؛ رهبرگ و گانزینگر، ۲۰۱۸: ۷۲). شبکه یکپارچه فرماندهی و کنترل، داده‌های رادارها را ترکیب و تصمیم‌گیری را خودکار می‌کند و هم‌افزایی لایه‌ها، توان پدافند را از سطح سامانه‌محور به شبکه‌ای ارتقا می‌دهد .

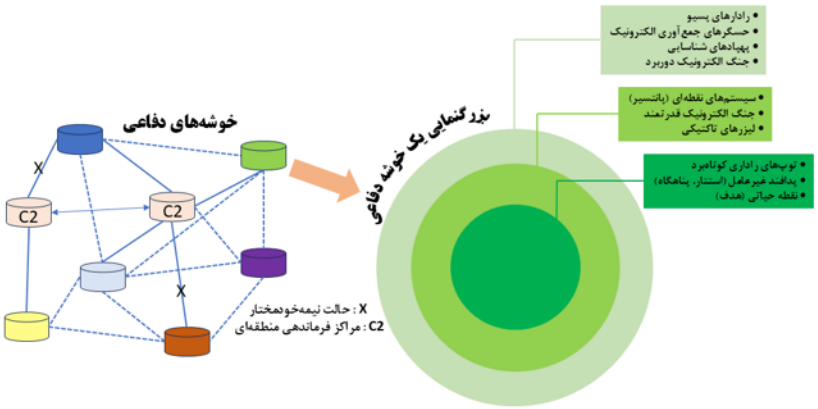
مدل پیشنهادی

در اینجا یک مدل پدافند هوایی تاب‌آور و تطبیق‌پذیر[1] (راد) برای محیط‌های دارای محدودیت پیشنهاد می‌شود:

مدل مفهومی: مدل مفهومی پیشنهادی برای سیستم چندلایه تطبیق‌پذیر با هسته تاب‌آور و معماری خوشه‌ای غیرمتمرکز در شکل ۱ ترسیم شده است. این مدل بر اساس چهار رکن اصلی (ساختاری، شناختی، تسلیحاتی، عملیاتی) و با الهام از سیستم‌های زیستی (زیست‌پذیر) طراحی شده است. هسته مرکزی (عامل هوشمند)، یک مغز متفکر اما غیرمتمرکز که فرماندهی و کنترل را بر عهده دارد. لایه‌های پیرامون هسته، ارکان چهارگانه مدل به صورت حلقه‌های به هم‌پیوسته هستند. خوشه‌های دفاعی (گره‌های عملیاتی) مانند سلول‌های یک موجود زنده، در سراسر جغرافیا پراکنده‌اند و هر یک دارای سه لایه دفاعی (بیرونی، میانی، درونی) هستند و در نهایت ، شبکه ارتباطی (سیستم عصبی)، یک شبکه توزیع‌شده است که خوشه‌ها را به هسته و به یکدیگر متصل می‌کند.



1 Resilient & Adaptive Air Defense (RAAD)



شکل ۱ . مدل مفهومی سیستم چندلایه تطبیق‌پذیر با هسته تاب‌آور و معماری خوشه‌ای غیرمتمرکز

فلسفه وجودی مدل پیشنهادی: مدل‌های پدافندی رایج (آمریکا، رژیم صهیونیستی) بر فرضیه دسترسی نامحدود به فناوری سطح بالا، بودجه کلان و برتری اطلاعاتی مطلق استوارند. این مدل‌ها برای کشورهایی با محدودیت‌های ساختاری (تحریم، وابستگی فناوری، بودجه محدود، تهدیدات جغرافیایی خاص) قابل تکرار نیستند. مدل راد با پذیرش اصل "عدم تقارن راهبردی" به دنبال ایجاد تاب‌آوری و تطبیق‌پذیری به جای دستیابی به یک "سپر غیرقابل نفوذ" ایده‌آل است. هدف غایی این مدل، افزایش هزینه تهاجم برای دشمن به میزانی غیرقابل تحمل، از طریق ترکیب هوشمندانه لایه‌های دفاعی، فناوری و تاکتیک است.

ارکان چهارگانه مدل:

رکن ساختاری: این مدل به‌جای تقلید از الگوی لایه‌بندی عمقی (نیازمند جغرافیای وسیع)، از خوشه‌های دفاعی حول نقاط حیاتی (شهرها، مراکز انرژی، پایگاه‌ها) استفاده می‌کند. هر خوشه یک سیستم پدافندی یکپارچه کوچک‌مقیاس با سه لایه متحدالمرکز است: ۱) لایه بیرونی (شناسایی و انکار) مبتنی بر رادارهای پسیو، حسگرهای الکترونیک ارزان‌قیمت، پهپادهای شناسایی و جنگ الکترونیک برای اخلال و انکار دسترسی دشمن در دوربرد؛ ۲) لایه میانی (رهگیری با چگالی بالا) از ترکیب سیستم‌های نقطه‌ای کوتاه‌برد (مانندPantsir) با سیستم‌های غیرسینتیک شامل جنگ الکترونیک ضد-پهپاد/موشک و لیزرهای تاکتیکی توان‌بالا؛ ۳) لایه درونی (آخرین

خط دفاع) شامل سیستم‌های بسیار کوتاه‌برد (توپ‌های راداری) و پدافند غیرعامل (استتار، پناهگاه). این معماری با پذیرش محدودیت جغرافیایی، منابع را بر اهداف باارزش متمرکز می‌کند. ساختار خوشه‌ای تاب‌آوری ایجاد می‌کند؛ نابودی یک خوشه کل سیستم را فلج نمی‌کند و امکان توسعه تدریجی بر اساس اولویت را فراهم می‌آورد.

رکن شناختی (مرکز فرماندهی و کنترل «هوشمند و غیرمتمرکز»): مدل راد به جای یک مرکز متمرکز عظیم (آسیب‌پذیر در مدل‌های غربی)، از شبکه مراکز فرماندهی منطقه‌ای هوشمند مبتنی بر هوش مصنوعی سبک و قابل استقرار در محیط‌های متحرک استفاده می‌کند. هر مرکز، داده‌های حسگرهای خوشه خود و خوشه‌های همسایه را پردازش و با الگوریتم‌های پیش‌بینی تهدید و تخصیص خودکار هدف، گزینه‌های عملیاتی را به اپراتور انسانی ارائه می‌دهد. در صورت قطع ارتباط با ستاد کل، این مراکز به طور نیمه‌خودمختار به مدیریت دفاع خوشه خود ادامه می‌دهند (مأموریت‌محوری). ساختار غیرمتمرکز، آسیب‌پذیری در برابر حملات سایبری و جنگ الکترونیک را کاهش و قابلیت زنده‌مانی سیستم را افزایش می‌دهد. استفاده از هوش مصنوعی سبک، وابستگی به ابررایانه‌ها را کاهش داده و برای کشورهای دارای تحریم فناوری قابل دسترس‌تر است.

رکن تسلیحاتی (ترکیب بهینه «سینتیک، الکترونیک، انرژی مستقیم»): این مدل با اجتناب از وابستگی صرف به موشک‌های گران‌قیمت (که در نظریه رقابت سالوو موجب فرسایش مدافع می‌شود)، نسبت بهینه هزینه-اثربخشی را تعریف می‌کند: ۱) در برابر تهدیدات ارزشمند (جنگنده‌های نسل ۵/۴ و موشک‌های بالستیک) از موشک‌های میان‌برد و دوربرد با راهبری ترکیبی (راداری فعال + ضدتشعشع) استفاده می‌شود. ۲) در برابر تهدیدات انبوه و ارزان (پهپادها و موشک‌های کروز)، اولویت با سلاح‌های غیرسینتیک و کم‌هزینه نظیر سیستم‌های جنگ الکترونیک (خنثی‌سازی همزمان چند هدف) و سلاح‌های پرتو مستقیم (لیزرهای توان‌بالا، مایکروویو) است. این ترکیب، اقتصاد رقابت سالوو را به نفع مدافع تغییر می‌دهد: رهگیری پهپاد ۲۰۰ دلاری با موشک ۵۰۰،۰۰۰ دلاری، مهاجم را به حملات ازدحامی تشویق می‌کند، اما رهگیری با لیزر با هزینه ۱۰ دلار، موازنه را برگردانده و تهاجم انبوه را بی‌صرفه می‌سازد. این قلب برتری مدل راد است.

رکن عملیاتی (راهبرد «دفاع فعال پیش‌دستانه چپ‌پرتاب[۱]»): مدل راد به جای انتظار منفعلانه برای پرتاب موشک دشمن، بر سه محور استوار است: ۱) شناسایی و هدف‌گیری چرخه تهاجم با استفاده از منابع اطلاعاتی (انسانی، سیگنالی، سایبری، ماهواره‌ای) برای کشف پرتابگرها و مراکز کنترل دشمن پیش از حمله. ۲) اقدام غیرسینتیک پیشدستانه شامل عملیات سایبری و جنگ الکترونیک برای خرابکاری در سامانه‌های دشمن، گمراه کردن یا انهدام پهپادها در آشیانه. ۳) آتش دوربرد با موشک‌ها یا پهپادهای تهاجمی برای انهدام زیرساخت‌های حمله در عمق خاک دشمن. این راهبرد، عمق دفاعی را از فضای خودی به فضای اطلاعاتی و فیزیکی دشمن گسترش می‌دهد و با خنثی‌سازی تهدید پیش از پرتاب، فشار بر لایه‌های رهگیری را کاهش می‌دهد.

مبانی نظری مدل پیشنهادی:

بر اساس چارچوب‌های نظری پیشین، مبانی مدل راد به شرح زیر استنتاج شده است:

۱ .نظریه سالوو: برتری به توان مدیریت حجم و اقتصاد درگیری وابسته است، نه کیفیت منفرد سامانه‌ها. معادله کلاسیک سالوو با افزایش هزینه دفاع نسبت به حمله، انگیزه مهاجم را بالا می‌برد. مدل راد با معکوس کردن این معادله (کاهش هزینه دفاع و افزایش هزینه حمله)، انگیزه تهاجم را کاهش می‌دهد. همچنین، به جای لایه‌بندی عمقی خطی، از لایه‌بندی خوشه‌ای همپوشان استفاده می‌کند که هر خوشه یک سیستم دفاعی خودمختار کامل است.

۲ .نظریه دفاع شبکه‌محور قابل تاب‌آوری: مدل راد از شبکه متمرکز ستاره‌ای به شبکه توزیع‌شده خوشه‌ای مهاجرت می‌کند و تأکید را از صرفاً اتصال‌پذیری به بقاپذیری تغییر می‌دهد. از نظریه سیستم‌های پیچیده تطبیق‌پذیر برای تعریف خوشه‌های دفاعی به عنوان عاملان مستقل، مراکز فرماندهی به عنوان سازوکار هماهنگی، و داده و هوش مصنوعی به عنوان حافظه جمعی بهره گرفته شده است.

۳. نظریه تاب‌آوری سایبر–فیزیکی: مدل راد تاب‌آوری همزمان در برابر حملات فیزیکی (موشک، پهپاد)، حملات سایبری (اختلال در فرماندهی) و حملات الکترونیک (اخلال در

---

۱ Proactive Left-of-Launch Defense : به مجموعه اقداماتی گفته می‌شود که هدف آن خنثی‌سازی تهدید موشکی قبل از لحظه شلیک است. به جای رهگیری موشک در هوا(Right-of-Launch)، این رویکرد تلاش می‌کند زنجیره آماده‌سازی، فرماندهی و کنترل، یا زیرساخت‌های پرتاب دشمن را مختل کند تا اساساً موشک هرگز شلیک نشود.

ارتباطات) را طراحی می‌کند. از نظریه بهینه‌سازی چندهدفه تحت محدودیت برای بهینه‌سازی همزمان سه مؤلفه استفاده شده است: حداکثرسازی احتمال رهگیری (اثربخشی)، حداقل‌سازی هزینه دفاع (اقتصادی) و حداکثرسازی بقاپذیری (تاب‌آوری)، با قید بودجه محدود و محدودیت‌های فناورانه.

تطبیق مدل پیشنهادی با ساختارهای دفاعی آمریکا، اسرائیل، چین و روسیه

الگوی دفاع شبکه‌ای و چندلایه پیشنهادی از منظر مؤلفه‌های اصلی با الگوهای کشورهای پیشرفته بصورت زیر قابل مقایسه است:

ایالات متحده: پدافند آمریکا مبتنی بر سامانه‌های متنوعی چون پاتریوت، تاد (موشک بالستیک)، AEGIS و SM-6 (تهدیدات هوایی) است. با وجود اثربخشی، هزینه بالای پاتریوت (۸۰۰ میلیون دلار سالانه برای ۱۵ گردان، بدون احتساب جایگزینی موشک‌ها) چالش اصلی است. به همین دلیل، آمریکا به سمت سامانه‌های ارزان‌تر مانند لیزرهای پرانرژی و تسلیحات مایکروویو برای مقابله اقتصادی با حملات سالوو حرکت کرده است.

رژیم صهیونیستی: پدافند این کشور بر لایه‌بندی دقیق استوار است: گنبد آهنین (کوتاه‌برد)، فلاخن داوود (میان‌برد) و پیکان (بلندبرد). استفاده از سامانه‌های هوابرد هشدار و رهگیری (پهپاد و هواپیما) برای افزایش زمان واکنش از ویژگی‌های برجسته آن است. مدل پیشنهادی با رویکرد مشابه، قابلیت ارائه پوشش دفاعی برای جغرافیای وسیع‌تر را دارد.

چین: ساختار A2/AD چین با هدف منع دسترسی آمریکا به شرق آسیا، ترکیبی از رادارهای هشدار سریع، موشک‌های پدافندی، جنگنده‌های نسل جدید و تعداد انبوه پهپاد (بیش از ۴۱ هزار سامانه تا ۲۰۲۳) است. تأکید بر لایه بیرونی با شبکه‌های راداری وسیع و سنسورهای هوابرد، الگویی مشابه با مدل پیشنهادی برای جبران ضعف در شناسایی تهدیدات کم‌ارتفاع است.

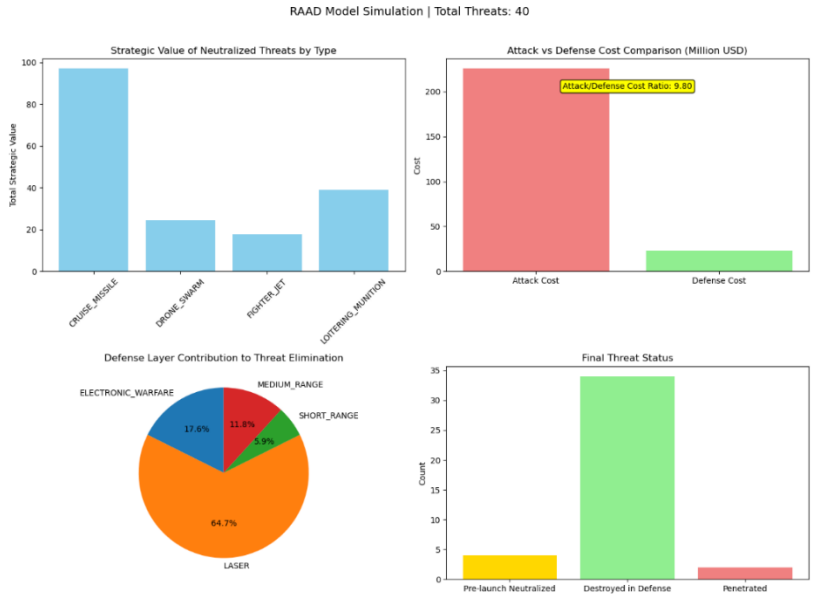
روسیه: پدافند روسیه ترکیبی از شبکه‌های راداری، سامانه‌های موشکی زمین‌پایه و هواپایه است. تمرکز این کشور بر تسلیحات تهاجمی مانند موشک اسکندر (۴۸۰ موشک در ده گردان)، کروز کالیبر و موشک‌های هایپرسونیک (کینژال) نشان‌دهنده توان عبور از دفاع‌های مرسوم است.

سیستم آمریکایی IAMD مبتنی بر AEGIS با دقت ۹۹٫۹٪ در شرایط ایده‌آل، دارای نقاط ضعف اساسی است بطوریکه هزینه ۳ میلیارد دلاری هر ناو، وابستگی به GPS و آسیب‌پذیری در

برابر جنگ الکترونیک است. مدل پیشنهادی به دلیل عدم وابستگی به زیرساخت‌های پیچیده و مراکز داده عظیم، تاب‌آوری بیشتری داشته و با قطع ارتباط مرکز، خوشه‌ها مستقل به کار ادامه می‌دهند. اقتصاد دفاعی نامتوازن و هزینه بالای رهگیری موشکی از چالش‌های اصلی رژیم صهیونیستی است. مدل پیشنهادی با بهره‌گیری از جنگ الکترونیک و لیزر، از طریق خوشه‌بندی، حجم تهدید را مدیریت و با حملات انبوه توزیع‌شده مقابله می‌کند. مدل S-400/500/Pantsir در روسیه با سلسله‌مراتب شدید و انعطاف‌ناپذیری (مشهود در اوکراین)، نیازمند زمان برای جابه‌جایی و آسیب‌پذیر در برابر حمله اولیه است. مدل پیشنهادی با خوشه‌های غیرمتمرکز، تحرک و پنهان‌کاری بالا (سیستم‌های کوچک‌مقیاس) و یادگیری تطبیقی، با هر درگیری هوشمندتر می‌شود. مدل HQ-9/HQ-19 با شبکه Skynet نیازمند زیرساخت ثابت و گسترده (هزاران پایگاه، فیبر نوری ملی، مراکز داده عظیم) و خاک امن برای استقرار در چین است. مدل پیشنهادی دارای استقلال جغرافیایی (کارایی در کشورهای کوچک)، قابلیت استقرار سریع و انعطاف‌پذیری بالا در تطبیق با جغرافیای مختلف است. مدل راد به جای تعقیب برتری فناورانه مطلق (الگوی قدرت‌های بزرگ)، بر تاب‌آوری، تطبیق‌پذیری و اقتصاد دفاعی هوشمند متمرکز است. با ترکیب ساختار خوشه‌ای غیرمتمرکز، تسلیحات KED (سینتیک-الکترونیک-انرژی مستقیم) و راهبرد چپ‌پرتاب داده‌محور، هزینه تهاجم برای دشمن را تا حد غیرقابل تحمل افزایش می‌دهد.

شبیه‌سازی مدل پیشنهادی

شبیه‌سازی مفهومی ساده از مدل راد در نرم‌افزار پایتون پیاده‌سازی شده است. کد این برنامه در سایت گیت‌هاب به آدرس https://github.com/ykhorrami/RAAD/tree/main قرار داده شده است. این کد ایده‌های اصلی مدل شامل خوشه‌بندی، ترکیب سلاح‌های انرژی مستقیم، جنگ الکترونیک، تأثیر راهبرد چپ‌پرتاب بر کاهش تلفات و هزینه اقتصادی را نمایش می‌دهد. خروجی‌های قابل مشاهده از اجرای شبیه‌سازی بصورت شکل ۲ است:



شکل ۲. خروجی شبیه‌سازی مدل راد شامل ۱) ارزش تهدیدات خنثی‌شده بر اساس نوع، ۲) مقایسه هزینه‌های حمله و دفاع، ۳) سهم هر لایه دفاعی در نابودی تهدیدات و ۴) وضعیت نهایی همه تهدیدات

خروجی شکل ۲ بیانگر ترکیبی از حملات پرتعداد کروز (ارزش بالا و هزینه متوسط)، حملات انبوه پهپاد (ارزش پایین و هزینه بسیار کم)، حملات جنگنده‌ها (ارزش بسیار بالا و هزینه بالا) و در نهایت حملات تراکمی پرسه‌زن‌ها (ارزش متوسط و هزینه کم) توسط دشمن است. همانطوریکه دیده می‌شود نسبت هزینه حمله به دفاع بگونه‌ای است که دفاع اقتصادی‌تر (کم‌هزینه‌تر) است که دلیل آن به سهم بالای استفاده از لیزر (هزینه عملیاتی کم علیه تهدیدات کوچک) و جنگ الکترونیک (هزینه کم علیه تهدیدات ارزان) و نیز استفاده از سلاح‌های کوتاه‌برد (هزینه متوسط) و میان‌برد (هزینه بالا) برمی‌گردد. تعداد خنثی‌شده پیش‌پرتاب نیز، بیانگر اثربخشی راهبرد چپ‌پرتاب است. ضمنا تعداد موارد پدافند شده بالا و میزان نفوذ تجهیزات دشمن به ساختار پدافندی بسیار محدود است. می‌توان پارامترها را برای سناریوهای مختلف تغییر داد. در این شبیه‌سازی از ۳ خوشه، ۴۰ تهدید، ترکیب تصادفی تهدیدات، سهم موفقیت اقدامی بالای ۸۰ درصد برای لیزر و جنگ‌الکترونیک و در نهایت نسبت تهدیدات کروز، پهپاد، جنگنده

و پرسه‌زن به ترتیب با نسبت ۰.۲، ۰.۴ ، ۰.۳ و ۰.۱ در شبیه‌سازی فرض شده است. از ۴۰ تهدید، قریب ۵ تهدید قبل از پرتاب خنثی شده (راهبرد چپ‌پرتاب)، ۳۲ تهدید توسط پدافند دفع شده و تنها ۳ تهدید عبور کرده است.

این برنامه یک نمایش مفهومی پویا از اصول مدل راد ارائه می‌دهد و می‌تواند به عنوان طرح اولیه برای شبیه‌سازی‌های پیچیده‌تر استفاده شود. برای واقعی‌تر شدن، می‌توان شبکه عصبی برای تصمیم‌گیری فرماندهی و کنترل، الگوریتم‌های بهینه‌سازی تخصیص هدف و مدل‌های فیزیکی دقیق‌تر را به آن اضافه کرد.

نتیجه‌گیری و پیشنهادها

پژوهش حاضر نشان داد که پارادایم کنونی پدافند هوایی در جهان، عمدتاً متأثر از الگوهای هزینه‌بر، متمرکز و وابسته به برتری فناورانه مطلق قدرت‌های بزرگ است. این الگوها برای اکثر کشورهای دارای محدودیت منابع، تحریم‌های فناورانه یا تهدیدات نامتقارن، غیرقابل تکرار، ناپایدار و شکننده هستند. در مقابل، مدل پیشنهادی در این مقاله (پدافند هوایی تاب‌آور و تطبیق‌پذیر) به عنوان یک چارچوب بدیع ارائه شد که بر سه اصل بنیادین استوار است: تاب‌آوری ساختاری (از طریق معماری خوشه‌ای غیرمتمرکز)، اقتصاد دفاعی هوشمند (از طریق ترکیب KED) و برتری شناختی (از طریق داده‌محوری و هوش مصنوعی سبک). این مدل ثابت می‌کند که می‌توان با پذیرش واقعیت محدودیت‌ها و بازتعریف معیارهای موفقیت (از نفوذناپذیری مطلق به تاب‌آوری و افزایش هزینه برای دشمن)، امنیت هوایی پایدار و مقرون‌به‌صرفه ایجاد کرد.

جهان در آستانه انقلابی در اندیشه دفاعی قرار دارد که از برتری مطلق به سمت تاب‌آوری هوشمند در حال حرکت است. مدل راد به عنوان یک نمونه نظری-عملیاتی نشان می‌دهد که آینده پدافند هوایی متعلق به سیستم‌هایی است که بتوانند محدودیت را به مزیت، تهدید را به فرصت یادگیری و هجوم را به فرسایش مهاجم تبدیل کنند. موفقیت در این مسیر مستلزم همکاری بین‌رشته‌ای (علوم نظامی، مهندسی، اقتصاد، علوم شناختی، علم داده و هوش‌مصنوعی) و جرأت بازاندیشی مفروضات دیرینه در مطالعات امنیتی است.

فهرست منابع

Barton, Geoffrey, & West, Philip, (2022), Air Defense Systems in the Age of Cyber and Hypersonic Threats, Modern Warfare Studies, 17(3), 60–80.

Bojicic-Dzelilovic, Vesna, (2023),The Evolution of Cruise Missiles and the Role of Air Defense Systems, Journal of Military Technology, 47(1), 45–60.

Hughes, W. P. (1995). Fleet Tactics and Coastal Combat. Naval Institute Press.

Byman, Daniel, (2021), Israel’s Use of Drones: A Case Study in Modern Air Warfare, Washington, DC: Brookings Institution.

Waltz, K. N. (1979). Theory of International Politics. Addison-Wesley.

Alberts, D. S., et al. (1999). Network Centric Warfare. CCRP

Miller, J. H., & Page, S. E. (2007). Complex Adaptive Systems. Princeton.

Linkov, I., & Kott, A. (2019). Cyber Resilience of Systems and Networks. Springer.

Deb, K. (2001). Multi-Objective Optimization using Evolutionary Algorithms. Wiley.

Kofman, M., & Fink, A. (2021). Escalation Management & the Ukrainian Drone War. Center for Naval Analysis.

Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. W. W. Norton & Company.

U.S. Department of Defense. (2020). Joint Publication 3-01: Countering Air and Missile Threats.

Acton, J. M. (2020). Re-thinking "Left of Launch" for Missile Defense. Carnegie Endowment for International Peace.

Brimley, S., et al. (2021). The Algorithmic Battlefield: AI and the Future of National Security. Center for a New American Security (CNAS).

Kott, A., & Perconti, P. (2018). Internet of Battle Things. Computer, 51(10), 70-75.

Futter, A., & Zala, B. (2021). Strategic hedging in the Middle East: The politics of missile defence. International Affairs, 97(2), 329-347.

Habibi, N., & Grare, F. (2020). Iran's Missile and Drone Forces: A Strategic Assessment. Carnegie Endowment for International Peace.

Cunningham, Fiona S., & Rainer, John, (2020),

The Future of Integrated Air Defense: A Multi-Layered Approach, Defense Studies Journal, 36(2), 102–118.

Deptula, David A, (2024), Fighting from the Inside: Air and Missile Defense of Forward Locations, Presentation delivered at the Air Warfare Symposium, Air & Space Forces Association (AFA), Orlando, Florida, February 20, 2024.

Gertler, Jeremiah, (2012), Air Defense Challenges Against Low-Cost Saturation Attacks, Washington, DC: Congressional Research Service (CRS).

Hassan, Mohammad, (2021), Iran’s Air Defense Systems and Their Challenges Against Modern Threats, Strategic Studies Journal, 30(1), 44–59.

Hutchinson, Matthew, (2017), The Case for Layered Defense Systems in Modern Warfare, Journal of Strategic Studies, 18(5), 67–90.

Ochmanek, David, (2017), Overcoming Anti-Access and Area Denial (A2/AD) Threats: Insights from War Games, Santa Monica, CA: RAND Corporation.

Rehberg, Carl R., & Gunzinger, Mark A, (2018), Air and Missile Defense at a Crossroads: New Concepts and Technologies to Defend America’s Overseas Bases, Washington, DC: Center for Strategic and Budgetary Assessments (CSBA).

Cancian, M. (2024). Air and Missile Defense in the Middle East: Lessons from Recent Conflicts. CSIS Institution.

Hinz, F. (2026). Iran's Missile Strike: A Technical Analysis of Operation True Promise 2. Arms Control Wonk. www.armcontrolwonk.com.

Rehberg, Carl R., & Gunzinger, Mark A, (2023), Air and Missile Defense at a Crossroads: New Concepts and Technologies to Defend America’s Overseas Bases, Washington, DC: Center for Strategic and Budgetary Assessments (CSBA).

International Institute for Strategic Studies (IISS). Iran's Air Defence Vulnerabilities Exposed. In Strategic Comments; IISS: London, 2025; Vol. 31.

Sheffi, Y. (2005). The resilient enterprise: Overcoming vulnerability for competitive advantage. The MIT Press.

Wong, K., & Speier, K. (2017). Low-Cost Missile Defense: Options for the Future. RAND Corporation.

Zabrodskyi, M. and others (2023). Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine. RUSI institution.