فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دهم، شماره دو، تابستان ۱۴۰۵

تدوین راهبردهای توسعه و پشتیبانی فناوری‌های سایبری در صنعت دفاعی با رویکرد تسریع چرخه تصمیم‌گیری فرماندهی و کنترل

علیرضا ابوالحسینی[۱]، محمد مهدی‌نژاد نوری[۲]، محمدرضا ولوی[۳]، سیدغلامحسن طباطبایی[۴]*

تاریخ دریافت: ۱۴۰۵/۰۴/۲۶ **تاریخ پذیرش: ۱۴۰۵/۰۷/۰۶**

چکیده

صنعت دفاعی در عصر تحول رقومی با پارادوکسی بنیادین مواجه است: از یک‌سو، ضرورت توسعه فناوری‌های پیشرفته سایبری برای ارتقای هوشمندی و دقت تسلیحات و تسریع چرخه تصمیم‌گیری فرماندهان، و از سوی دیگر، لزوم مصون‌سازی این تجهیزات در برابر تهدیدات روزافزون سایبری. این پژوهش با هدف تدوین مجموعه‌ای از راهبردهای کلان، راهبردهای عملیاتی، راهکارهای اساسی و الگوی نظارت برای توسعه و پشتیبانی فناوری‌های سایبری در صنعت دفاعی انجام شده است. با استفاده از روش تحقیق آمیخته اکتشافی متوالی [۱]، ابتدا با تحلیل مضمون اسناد معتبر بین‌المللی [۲]، ده فناوری شالوده‌شکن شناسایی و مضمون «ارتقای هوشمندی و امنیت در چرخه فرماندهی و کنترل با استفاده از فناوری‌های نوظهور سایبری» به‌عنوان قطب‌نمای پژوهش استخراج گردید. سپس با بهره‌گیری از روش دلفی سه‌مرحله‌ای (مشارکت ۵۰ خبره) و تحلیل مفهومی ماتریس سوات [۳]، موقعیت راهبردی صنعت دفاعی در ناحیه «تدافعی-پویا» تعیین شد. خروجی پژوهش در چهار سطح تدوین گردیده است: (۱) راهبردهای کلان در چهار محور بازآفرینی نهادی، خوداتکایی فناورانه، توانمندسازی سرمایه انسانی و تاب‌آوری اقتصادی؛ (۲) راهبردهای عملیاتی در قالب هفت خوشه معنایی شامل تصمیم‌یارهای هوشمند، امنیت ارتباطات، سامانه‌های خودمختار، پایش و شناسایی پیشرفته، حاکمیت داده و استانداردسازی، آموزش و توانمندسازی، و یکپارچه‌سازی فرماندهی و کنترل؛ (۳) راهکارهای اساسی در چهار حوزه نهادی، منابع انسانی، زیرساخت و تأمین مالی؛ (٤) الگوی نظارت سه‌سطحی با شاخص‌های جهت‌دهنده که امکان بازخورد مستمر و اصلاح راهبردها را فراهم می‌آورد. این مجموعه راهبردها و الگوی نظارت، به‌عنوان نقشه‌راهی برای سیاست‌گذاران دفاعی در جهت گذر از نگاه جزیره‌ای به رویکرد یکپارچه و پویا قابل استفاده است [۷]. نوآوری اصلی مقاله، ارائه مجموعه‌ای منسجم از راهبردها و الگوی نظارت است که با تمرکز بر تسریع چرخه تصمیم‌گیری فرماندهان [۸]، شکاف میان توسعه و امنیت را در صنعت دفاعی کشور پر می‌کند.

واژگان کلیدی: چرخه تصمیم‌گیری **OODA**، فرماندهی و کنترل، جنگ شبکه‌محور، آگاهی وضعیتی، سامانه‌های **ISR&C**، چارچوب راهبردی پویا، فناوری‌های سایبری دفاعی، خوداتکایی فناورانه.

[۱] دانشجوی مقطع دکتری (دانشگاه عالی دفاع ملی)

[۲] استاد دانشگاه عالی دفاع ملی – استاد راهنما و نویسنده مسئول

[۳] دانش‌یار دانشگاه صنعتی مالک اشتر

[٤] استادیار دانشگاه صنعتی مالک اشتر

[Downloaded from ic4i-journal.ir on 2026-11-21]

۱. کلیات

۱.۱. مقدمه و بیان مسئله

جهان امروز، شاهد یکی از سریع‌ترین و شالوده‌شکن‌ترین دوره‌های تحول فناوری در تاریخ بشر است. همگرایی هوش مصنوعی، محاسبات کوانتومی، اینترنت اشیا و سامانه‌های خودمختار، نه‌تنها صنایع غیرنظامی، بلکه زیرساخت‌های دفاعی و امنیتی کشورها را دستخوش دگرگونی‌های بنیادین کرده است[۴]. در این میان، فضای سایبر به‌عنوان «عرصه پنجم نبرد» (پس از زمین، هوا، دریا و فضا)، نقشی دوگانه ایفا می‌کند: از یک‌سو بستر ظهور قابلیت‌های تحول‌آفرین مانند تسلیحات هوشمند، فرماندهی شبکه‌محور و آگاهی وضعیتی لحظه‌ای است[۵]، و از سوی دیگر، خود به‌عنوان میدان نبردی مستقل، محل تقابل پیچیده‌ای از حملات سایبری، جاسوسی رقومی و جنگ شناختی محسوب می‌شود[۶]. این دوگانگی، صنعت دفاعی را در برابر پرسشی راهبردی قرار داده است: چگونه می‌توان ضمن بهره‌مندی از فرصت‌های بی‌نظیر فناوری‌های سایبری، تاب‌آوری و امنیت سامانه‌ها را در برابر تهدیدات نوظهور تضمین کرد؟ پاسخ به این پرسش، مستلزم فراتر رفتن از برنامه‌ریزی‌های صرفاً خطی و بخشی‌نگر است. رویکردهای سنتی که یا صرفاً بر «توسعه» متمرکزند (غافل از آسیب‌پذیری‌های سایبری) و یا صرفاً بر «پدافند» (غافل از ضرورت نوآوری و هم‌افزایی)، در مواجهه با ماهیت ترکیبی و پویای تهدیدات امروز، کارایی خود را از دست داده‌اند[۷]. آنچه ضرورت دارد، طراحی چارچوبی است که بتواند از سطح کلان‌ترین جهت‌گیری‌های راهبردی (که در این پژوهش از آن با عنوان «مضمون فراگیر» یاد می‌شود) تا جزئی‌ترین اقدامات اجرایی را در یک زنجیره علّی-معلولی منسجم، به هم متصل سازد و هم‌زمان، امکان بازنگری و اصلاح مستمر را از طریق حلقه‌های بازخورد فراهم آورد.

مسئله اصلی این پژوهش، فقدان چنین چارچوبی در صنعت دفاعی کشور است. بررسی‌های اولیه نشان می‌دهد که علی‌رغم پیشرفت‌های قابل‌توجه در حوزه‌های موشکی، پهپادی و الکترونیک، هنوز یک «نقشه راه یکپارچه» برای توسعه و پشتیبانی فناوری‌های سایبری در سطح کلان صنعت دفاعی تدوین نشده است[۱۱]. این فقدان، خود را در عواملی چون موازی‌کاری دستگاه‌های متولی، عدم شفافیت در اولویت‌بندی پروژه‌های فناورانه، ضعف در جذب و نگهداشت نخبگان، و آسیب‌پذیری سامانه‌های موجود در برابر حملات سایبری نشان می‌دهد[۱۲]. بعلاوه بررسی فرامین و منویات قائد شهید قدس سره الشریف هم نشان میدهد ایشان بصورت مستمر و با تاکید فوق‌العاده در زمینه بهره‌مندی از فناوری های نوظهور از جمله هشو مصنوعی، کوانتوم، سایبر و ... در عرصه های مختلف از جمله در عرصه های نظامی توصیه های اکیدی داشته اند.[۱۸] بنابراین، این پژوهش در صدد است تا با بهره‌گیری از روش‌شناسی ترکیبی، چنین چارچوبی را طراحی و اعتبارسنجی کند و در نهایت، آن را به‌عنوان ابزاری برای سیاست‌گذاری و تصمیم‌گیری در اختیار مدیران ارشد صنعت دفاعی قرار دهد.

امروزه، تسریع چرخه تصمیم‌گیری[۲] در سامانه‌های فرماندهی و کنترل، به‌عنوان یک اصل راهبردی در جنگ‌های شبکه‌محور شناخته می‌شود و فناوری‌های سایبری ابزار اصلی نیل به این هدف هستند. با توجه به ماهیت پیچیده و پویای تهدیدات سایبری، هر گونه تأخیر در فرآیند تصمیم‌گیری می‌تواند به از دست دادن برتری راهبردی منجر شود. از این‌رو، چارچوب راهبردی توسعه فناوری‌های سایبری باید به‌گونه‌ای طراحی شود که ضمن هوشمندسازی و مصون‌سازی تجهیزات دفاعی، به‌طور مستقیم به بهبود حلقه‌های فرماندهی و کنترل و تسریع چرخه تصمیم‌گیری بیانجامد.

۲. مبانی نظری و چارچوب مفهومی

۱.۲. پارادایم جنگ سایبری و الزامات راهبردی آن

درک ماهیت جنگ‌های معاصر، نقطه عزیمت هر گونه برنامه‌ریزی راهبردی در حوزه دفاع است. نظریه‌پردازان نظامی، از اواخر دهه ۱۹۹۰ با معرفی مفهوم «جنگ شبکه‌محور»[۳][۵]، اعلام کردند که برتری در میدان نبرد دیگر صرفاً در گرو انباشت تجهیزات و آتش‌افشانی نیست، بلکه توانایی «تولید، توزیع و بهره‌برداری از اطلاعات» در زمان سریع‌تر از دشمن، به‌عنوان عامل کلیدی پیروزی مطرح می‌شود. این پارادایم، بعدها با

[۲] OODA Loop

[۳] Network-Centric Warfare

[Downloaded from ic4i-journal.ir on 2026-11-21]

مفاهیمی چون «جنگ ترکیبی»[۴] و «عملیات چندعرصه‌ای»[۵] تکمیل شد و بر این نکته تأکید یافت که میدان نبرد امروز، تلفیقی درهم‌تنیده از عرصه‌های فیزیکی (زمین، هوا، دریا) و غیرفیزیکی (سایبری، اطلاعاتی/شناختی) است[۱۰].

در این میان، فضای سایبر نقشی محوری دارد. این فضا نه تنها بستری برای عملیات‌های تهاجمی و تدافعی مستقل است، بلکه به‌عنوان «چسب اتصال» سایر عرصه‌ها عمل می‌کند؛ به‌گونه‌ای که اختلال در شبکه‌های ارتباطی و اطلاعاتی، می‌تواند کل یک عملیات نظامی را با شکست مواجه سازد[۶]. از این منظر، فناوری‌های سایبری را باید به‌عنوان «عامل توانمندساز»[۶] تمامی ابعاد قدرت دفاعی در نظر گرفت[۱۳]. بنابراین، هر گونه راهبرد توسعه در این حوزه، باید به‌طور هم‌زمان به «ارتقای قابلیت‌های تهاجمی/تدافعی در فضای سایبر» و «مصون‌سازی سامانه‌های فیزیکی در برابر تهدیدات سایبری» بپردازد[۱۵].

۲.۲. پیشینه پژوهش‌های مرتبط با تدوین راهبردهای توسعه فناوری سایبری

بررسی پیشینه پژوهش نشان می‌دهد که اگرچه مطالعات متعددی در حوزه فناوری‌های سایبری و صنعت دفاعی انجام شده، اما پژوهشی که به‌طور جامع به تدوین راهبردهای کلان، راهبردهای عملیاتی و الگوی نظارت برای توسعه و پشتیبانی فناوری‌های سایبری در صنعت دفاعی کشور پرداخته باشد، یافت نشد.

مطالعات مشابه عمدتاً بر جنبه‌های زیر متمرکز بوده‌اند: (۱) شناسایی و اولویت‌بندی فناوری‌های نوظهور در حوزه دفاع (مانند گزارش‌های ناتو، سازمان دفاعی اروپا و وزارت دفاع آمریکا)؛ (۲) تحلیل نقاط قوت، ضعف، فرصت‌ها و تهدیدهای صنعت دفاعی در حوزه فناوری (چندین پایان‌نامه و مقاله داخلی)؛ (۳) بررسی نقش فناوری اطلاعات و ارتباطات در دفاع دانش‌بنیان؛ (٤) عوامل مؤثر بر نوآوری فناورانه در واحدهای صنعتی دفاعی؛ (۵) مطالعات تطبیقی ساختار رزم سایبری کشورهای هدف. اما حلقه مفقوده در این پژوهش‌ها، عدم ارائه مجموعه‌ای یکپارچه از راهبردها در سطوح مختلف (کلان و عملیاتی) به همراه راهکارهای اجرایی و الگوی نظارت است. پژوهش حاضر، این خلأ را با ارائه مجموعه‌ای منسجم از راهبردها و الگوی نظارت پر می‌کند.

۳.۲. ضرورت چارچوب‌های برنامه‌ریزی پویا در صنایع دفاعی

برنامه‌ریزی راهبردی در صنعت دفاعی، با چالش‌های منحصربه‌فردی مواجه است که آن را از برنامه‌ریزی در صنایع غیرنظامی متمایز می‌کند. بلندمدت بودن افق سرمایه‌گذاری، هزینه‌های سنگین تحقیق و توسعه، محرمانگی بالا، و وابستگی شدید به تحولات ژئوپلیتیک، همگی ضرورت اتخاذ رویکردهایی را ایجاب می‌کنند که از انعطاف‌پذیری و قابلیت بازنگری بالایی برخوردار باشند. متأسفانه، بسیاری از مدل‌های کلاسیک برنامه‌ریزی راهبردی (مانند مدل هاروارد یا مدل سوات ساده)، اگرچه برای تشخیص موقعیت اولیه مفیدند، اما فاقد سازوکارهای لازم برای «یادگیری سازمانی» و «انطباق با تغییرات سریع محیطی» هستند[۹].

به همین دلیل، در دهه اخیر، رویکردهای نوینی مانند «برنامه‌ریزی مبتنی بر سناریو»[۷] «مدیریت پویا»[۸] و «چارچوب‌های حلقه‌بسته»[۹] در ادبیات دفاعی مورد توجه قرار گرفته‌اند. ویژگی مشترک این رویکردها، تأکید بر «بازخورد» به‌عنوان موتور محرک اصلاح و بهبود مستمر است. به‌عبارتی، برنامه‌ریزی راهبردی در این نگاه، یک فرایند خطی با نقطه شروع و پایان مشخص نیست، بلکه یک چرخه دائمی از «اقدام، سنجش، یادگیری و اصلاح» محسوب می‌شود. پژوهش حاضر، با الهام از این رویکردهای نوین، سعی دارد چارچوبی ارائه دهد که در آن، تمامی عناصر از مضمون فراگیر گرفته تا شاخص‌های عملکردی، در یک زنجیره بازخوردی منسجم قرار گیرند.

٤.۲. مضمون فراگیر به‌عنوان «قطب‌نمای راهبردی»

[۴] Hybrid Warfare

[۵] Multi-Domain Operations

[۶] Enabler

[۷] Scenario Planning

[۸] Dynamic Management

[۹] Closed-Loop Frameworks

[Downloaded from ic4i-journal.ir on 2026-11-21]

در این پژوهش، مضمون فراگیر[10] به‌عنوان «بنیان‌گذار جهت‌گیری کلی» و «معیار سنجش هم‌راستایی» تمامی عناصر چارچوب، انتخاب شده است. این مضمون که حاصل تحلیل عمیق اسناد راهبردی و با تأکید بر مفاهیم فرماندهی و کنترل است، عبارت می‌باشد از: «**ارتقای هوشمندی و امنیت در چرخه فرماندهی و کنترل با استفاده از فناوری‌های نوظهور سایبری**». این مضمون، سه رکن اساسی را در بر می‌گیرد. رکن نخست، هوشمندی در چرخه فرماندهی و کنترل است که به‌معنای تسریع مراحل حلقه تصمیم‌گیری (مشاهده-جهت‌گیری-تصمیم-اقدام) از طریق به‌کارگیری فناوری‌هایی چون هوش مصنوعی، کلان‌داده و شبکه‌های عصبی می‌باشد[۸]. رکن دوم، امنیت در چرخه فرماندهی و کنترل است که به‌معنای مصون‌سازی ارتباطات، داده‌ها و تصمیمات فرماندهان در برابر حملات سایبری، اختلالات الکترومغناطیسی و جنگ شناختی بوده و با استفاده از رمزنگاری پیشرفته، معماری‌های اعتمادصفر، بلاک‌چین و سامانه‌های تشخیص نفوذ تحقق می‌یابد. رکن سوم، یکپارچگی سامانه‌های ISR&C است که به‌معنای اتصال و هماهنگی تمامی سامانه‌های فرماندهی، کنترل، ارتباطات، رایانش، اطلاعات، نظارت و شناسایی در قالب یک معماری منسجم و خدمت‌گرا می‌باشد.

اهمیت این مضمون در آن است که به‌عنوان «قطب‌نمای راهبردی»، تمامی مراحل بعدی پژوهش را جهت‌دهی می‌کند. بدین معنا که هر راهبرد کلان، هر راهبرد عملیاتی، هر راهکار اساسی و هر شاخص ارزیابی، باید پاسخگوی این سوال بنیادین باشد که: «آیا این اقدام، به تحقق هوشمندی و امنیت تجهیزات نظامی در چرخه فرماندهی و کنترل کمک می‌کند یا خیر؟» این رویکرد، از انحراف پروژه‌ها و اقدامات به سمت اهداف غیرمرتبط یا کم‌اولویت جلوگیری کرده و وحدت رویه را در سطح کلان صنعت دفاعی تضمین می‌کند.

در این میان، مفاهیم فرماندهی و کنترل[11] به‌عنوان قلب تپنده هر سیستم نظامی، نقشی محوری در بهره‌مندی از فناوری‌های سایبری ایفا می‌کنند. حلقه تصمیم‌گیری (مشاهده-جهت‌گیری-تصمیم-اقدام) که توسط سرهنگ جان بوید برای توصیف فرآیند تصمیم‌گیری در نبردهای هوایی ارائه شد، امروزه به‌عنوان چارچوبی کلیدی برای تحلیل و بهبود سامانه‌های فرماندهی و کنترل در جنگ‌های شبکه‌محور و سایبری مورد استفاده قرار می‌گیرد. سرعت و دقت در چرخش این حلقه، مستقیماً با کیفیت تصمیم‌گیری فرماندهان و در نهایت، پیروزی در میدان نبرد ارتباط دارد. فناوری‌های سایبری، به‌ویژه هوش مصنوعی و کلان‌داده، می‌توانند با تسریع فرآیندهای جمع‌آوری، پردازش و تحلیل اطلاعات، طول این حلقه را به‌شدت کاهش دهند و به فرماندهان امکان دهند تا سریع‌تر از دشمن اقدام کنند. از این منظر، چارچوب راهبردی توسعه فناوری‌های سایبری در صنعت دفاعی، باید با هدف ارتقای توانمندی‌های فرماندهی و کنترل و بهبود آگاهی وضعیتی فرماندهان در تمامی عرصه‌های نبرد طراحی شود.[۱۶]

بطور خلاصه مضمون "ارتقای هوشمندی و امنیت در چرخه فرماندهی و کنترل با استفاده از فناوری‌های نوظهور سایبری"، سه رکن اساسی را در بر می‌گیرد: (۱) هوشمندی در چرخه فرماندهی و کنترل (تسریع حلقه**OODA**)؛ (۲) امنیت در چرخه فرماندهی و کنترل (مصون‌سازی در برابر حملات سایبری)؛ (۳) یکپارچگی سامانه‌های **ISR&C** (اتصال و هماهنگی تمامی سامانه‌ها). تمامی راهبردهای تدوین‌شده در این پژوهش، در راستای تحقق این مضمون فراگیر طراحی شده‌اند.

۳. روش‌شناسی تحقیق

پژوهش حاضر از روش تحقیق آمیخته اکتشافی متوالی (کیفی ← کمی) استفاده کرده است. در مرحله کیفی، ابعاد و مؤلفه‌های مسئله (فناوری‌ها، عرصه‌های نبرد، عوامل محیطی) استخراج و مضمون فراگیر شناسایی شد. در مرحله کمی، با مشارکت خبرگان، اعتبارسنجی و اولویت‌بندی انجام و راهبردها و الگوی نظارت تدوین گردید.

۱.۳. رویکرد کلی و منطق انتخاب آن

[10] Overarching Theme

[11] Command and Control - C۲

[Downloaded from ic4i-journal.ir on 2026-11-21]

با توجه به ماهیت چندبعدی موضوع و نیاز به ترکیب «کشف» (برای شناسایی مؤلفه‌های نوین) و «اعتبارسنجی» (برای تأیید کاربردپذیری آنها در بافت بومی)، پژوهش حاضر از روش تحقیق آمیخته اکتشافی متوالی استفاده کرده است. دلیل انتخاب این روش، آن است که ابتدا باید با مرور عمیق ادبیات و اسناد، ابعاد و مؤلفه‌های مسئله (فناوری‌ها، عرصه‌های نبرد، عوامل محیطی) استخراج شوند (مرحله کیفی) و سپس با مشارکت خبرگان، اعتبار مفهومی آنها و همچنین اولویت‌های راهبردی مورد تأیید قرار گیرند. در نهایت، بر اساس این یافته‌ها، چارچوب نهایی طراحی و شاخص‌های نظارت تدوین می‌شوند.

۲.۳. مرحله کیفی: تحلیل مضمون و استخراج مؤلفه‌ها

در مرحله کیفی، با استفاده از روش تحلیل مضمون و بر اساس مدل شش مرحله‌ای براون و کلارک (۲۰۰۶)، به بررسی و کدگذاری اسناد و متون پرداخته شد. جامعه اسنادی این مرحله شامل چهار دسته منابع بود: (۱) اسناد معتبر بین‌المللی شامل گزارش‌های راهبردی ناتو، سازمان دفاعی اروپا، وزارت دفاع آمریکا، مرکز مطالعات راهبردی و بین‌المللی و اتحادیه اروپا؛ (۲) اسناد بالادستی صنعت دفاعی کشور نظیر قانون برنامه هفتم توسعه، سند جامع علم‌وفناوری دفاعی و برنامه‌های ارائه‌شده توسط وزرای دفاع؛ (۳) مقالات علمی معتبر در پایگاه‌های داده (**Science Direct, Springer, Emerald**) با کلیدواژه‌های مرتبط؛ و (٤) آموزه‌های دینی و فرمایشات امامین انقلاب در حوزه ضرورت ارتقای قدرت دفاعی.

فرایند تحلیل مضمون در چهار گام انجام شد. گام اول، کدگذاری اولیه بود. گام دوم، دسته‌بندی کدها در مضامین اولیه بود. گام سوم، سازماندهی مضامین اولیه در قالب مضامین سازمان‌دهنده بود. در نهایت، در گام چهارم، مضمون فراگیر پژوهش استخراج شد.

جدول ۱. فرآیند تحلیل مضمون و استخراج مضامین.

مضامین اولیه	مضامین سازمان‌دهنده	مضمون فراگیر
• بهبود سرعت و دقت در جمع‌آوری و تحلیل داده‌ها • تسریع فرآیندهای تصمیم‌گیری در سطوح مختلف فرماندهی • کاهش خطاهای انسانی در چرخه مشاهده جهت‌گیری-تصمیم-اقدام • افزایش دقت در شناسایی و پیش‌بینی تهدیدات • خودکارسازی فرآیندهای پردازش اطلاعات	کارایی و هوشمندسازی چرخه تصمیم‌گیری	ارتقای هوشمندی و امنیت در چرخه فرماندهی و کنترل (C²) با استفاده از فناوری‌های نوظهور سایبری
• یکپارچه‌سازی سامانه‌های فرماندهی و کنترل • اتصال و هماهنگی بین سامانه‌های تسلیحاتی و حسگرها • ایجاد شبکه‌های ارتباطی امن و پایدار • مدیریت یکپارچه داده‌های میدان نبرد • قابلیت هم‌افزایی بین سامانه‌های C٤ISR	یکپارچگی و اتصال سامانه‌های C٤ISR	
• توسعه سامانه‌های خودمختار و هوشمند • توانایی واکنش سریع و خودکار در شرایط بحرانی • کاهش وابستگی به نیروی انسانی در عملیات خطرناک • ارتقای قابلیت‌های عملیاتی بااستفاده ازهوش مصنوعی • بهبود عملکرد پهپادها و ربات‌های نظامی	خودمختاری و توسعه هوش مصنوعی در دفاع	

[Downloaded from ic4i-journal.ir on 2026-11-21]

مضامین اولیه	مضامین سازمان‌دهنده	مضمون فراگیر
• بهینه‌سازی مصرف منابع و تجهیزات نظامی • کاهش هزینه‌های عملیاتی و نگهداری • مدیریت کارآمد زنجیره تأمین دفاعی • افزایش بهره‌وری در فرآیندهای پشتیبانی • استفاده بهینه از زیرساخت‌های اطلاعاتی	بهره‌وری و بهره‌وری در عملیات دفاعی	
• رمزنگاری پیشرفته و امنیت ارتباطات در چرخه فرماندهی و کنترل • تاب‌آوری در برابر حملات سایبری و جنگ شناختی • تشخیص و پیشگیری از نفوذ به سامانه‌های فرماندهی • حفاظت از داده‌های حساس عملیاتی • استقرار معماری اعتمادصفر در شبکه‌های نظامی	افزایش امنیت و اعتمادپذیری سایبری	

هم‌زمان با این فرایند، ده فناوری سایبری که در اسناد بین‌المللی به‌عنوان اولویت‌های شالوده‌شکن تا افق ۲۰۴۰ معرفی شده‌اند، شناسایی و با تأیید خبرگان، به‌عنوان فناوری‌های منتخب پژوهش انتخاب شدند.[۱۷]

۳.۳. مرحله کمی کیفی‌شده: روش دلفی و تحلیل سوات

در این مرحله، به‌جای تأکید بر محاسبات عددی و ضرایب وزنی دقیق، از روش دلفی سه‌مرحله‌ای با رویکرد «دستیابی به اجماع معنایی» استفاده شد. جامعه آماری این مرحله، ۵۰ خبره از چهار گروه تخصصی بودند: مدیران فناوری و نوآوری (۱۷ نفر)، مدیران آشنا با صحنه نبرد (۱۶ نفر)، متخصصان حوزه سایبری (۹ نفر) و آینده‌پژوهان (۸ نفر). انتخاب خبرگان با روش نمونه‌گیری هدفمند (قضاوتی) و بر اساس معیارهایی چون حداقل ۸ سال سابقه کاری مرتبط، تجربه در پروژه‌های کلان فناورانه و آشنایی با حوزه فناوری‌های سایبری و صحنه نبرد انجام شد. در مرحله اول دلفی، پرسشنامه‌ای شامل ۵۰ سؤال ماتریسی (۱۰ فناوری در ۵ عرصه نبرد) با طیف لیکرت سه‌درجه‌ای (کم، متوسط، زیاد) در اختیار خبرگان قرار گرفت تا شدت کاربرد هر فناوری در هر عرصه را ارزیابی کنند. همچنین، در بخش باز پرسشنامه، از خبرگان خواسته شد تا نقاط قوت، ضعف، فرصت‌ها و تهدیدهای هر یک از فناوری‌ها را در عرصه‌های مختلف، به‌صورت توصیفی و مفهومی، بیان نمایند.

در مرحله دوم دلفی، نتایج مرحله اول (به‌صورت میانگین و توزیع پاسخ‌ها) به همراه پرسشنامه بازنگری‌شده، در اختیار همان خبرگان قرار گرفت و از آن‌ها خواسته شد تا ضمن مرور نتایج گروهی، اولویت‌بندی کیفی خود را ارائه دهند. در این مرحله، بحث‌های مفهومی عمیقی در مورد «چرایی» اولویت‌بندی‌ها شکل گرفت و زمینه برای دستیابی به اجماع معنایی فراهم آمد. در مرحله سوم دلفی، خلاصه‌ای از یافته‌های مرحله دوم (شامل اولویت‌بندی‌های نهایی و یافته‌های جدید) مجدداً به خبرگان ارائه و میزان موافقت آن‌ها با این اولویت‌بندی‌ها در مقیاس لیکرت پنج‌درجه‌ای (کاملاً موافق تا کاملاً مخالف) سنجیده شد. نرخ توافق نهایی، با میانگین ٪۸۸.۷، نشان‌دهنده اجماع قوی در میان خبرگان بود.

هم‌زمان با فرایند دلفی، تحلیل سوات کیفی نیز انجام شد. در این تحلیل، از رویکرد «جهت‌دهی مفهومی» استفاده شد[۳]. بدین‌معنا که با تکیه بر نظرات خبرگان و تحلیل محتوایی پرسشنامه‌های تخصصی، موقعیت کلی صنعت دفاعی در حوزه فناوری‌های سایبری تعیین گردید. این تشخیص، پایه و اساس تدوین راهبردهای کلان قرار گرفت.

٤. یافته‌های پژوهش

۱.٤. مضمون فراگیر و نقش آن در هدایت تحلیل محیطی

فرایند تحلیل مضمون در چهار گام انجام شد. گام اول، کدگذاری اولیه بود که طی آن، ۲٤۰ کد اولیه از دل متون استخراج شد. گام دوم، دسته‌بندی کدها در مضامین اولیه بود که منجر به شکل‌گیری ۲۷ مضمون اولیه گردید. گام سوم، سازماندهی مضامین اولیه در قالب مضامین سازمان‌دهنده بود که نهایتاً به ۵ مضمون سازمان‌دهنده (شامل «کارایی و هوشمندسازی چرخه تصمیم‌گیری»، «یکپارچگی و اتصال سامانه‌های **ISR٤C**»، «خودمختاری و توسعه هوش مصنوعی در دفاع»، «مدیریت و

[Downloaded from ic4i-journal.ir on 2026-11-21]

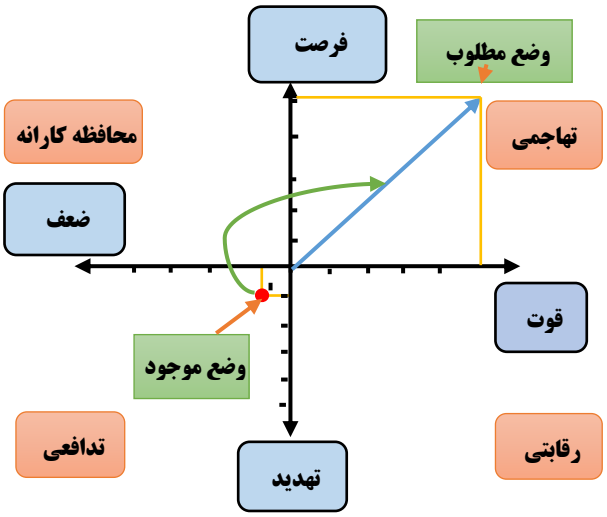
بهره‌وری در عملیات دفاعی» و «افزایش امنیت و اعتمادپذیری سایبری») انجامید. در نهایت، در گام چهارم، مضمون فراگیر پژوهش با عنوان «**ارتقای هوشمندی و امنیت در چرخه فرماندهی و کنترل با استفاده از فناوری‌های نوظهور سایبری**» استخراج شد که به‌عنوان یک «دستور کار راهبردی» عمل کرده و تمامی یافته‌های بعدی را جهت‌دهی کرده است. در فرایند تحلیل محیط داخلی، این مضمون به‌عنوان «فیلتری مفهومی» عمل کرد؛ بدین‌معنا که از میان انبوهی از نقاط قوت و ضعف احتمالی، تنها آن دسته از عواملی مورد توجه قرار گرفتند که با این مضمون ارتباط مستقیم داشتند. برای نمونه، در بخش نقاط قوت، عواملی چون «سرمایه‌های انسانی جوان و نخبه» و «توان علمی در توسعه محصولات نرم‌افزاری دفاعی» به‌عنوان قوت‌های اصلی شناسایی شدند، زیرا هر دو به‌طور مستقیم به «هوشمندی» کمک می‌کنند. همچنین در بخش نقاط ضعف، «وابستگی به فناوری خارجی و آسیب‌پذیری‌های مهم امنیتی» و «کمبود نیروی انسانی متخصص» در صدر قرار گرفتند، زیرا مستقیماً با رکن «امنیت» در تضاد هستند. این رویکرد، از پراکندگی و نامرتبط‌شدن عوامل محیطی جلوگیری کرده و تحلیل را متمرکز بر هدف اصلی نگه داشته است.

همچنین در بررسی اولویت فناوری های سایبری، ده فناوری سایبری که در اسناد بین‌المللی به‌عنوان اولویت‌های شالوده‌شکن تا افق ۲۰۴۰ معرفی شده‌اند، شناسایی و با تأیید خبرگان، به‌عنوان فناوری‌های منتخب پژوهش انتخاب شدند.[۱۷] این ده فناوری عبارتند از: هوش مصنوعی، کلان‌داده، سامانه‌های خودمختار، رابط کاربری انسان-ماشین، اینترنت اشیا، رایانش ابری (مه و لبه)، سامانه‌های فیزیکی_سایبری[۱۲]، سنجش مجتمع و سایبر، بلاک‌چین و فناوری کوانتوم. همچنین، بر اساس ادبیات موضوع، پنج عرصه نبرد (زمینی، هوایی، دریایی، سایبری و اطلاعاتی/شناختی) به‌عنوان عرصه‌های تأثیرپذیر از این فناوری‌ها، شناسایی گردیدند.[۱۴]

۲.۴. تحلیل موقعیت راهبردی (کیفی)

با انجام تحلیل سوات کیفی با تکیه بر نظرات خبرگان و تحلیل محتوایی پرسشنامه‌های تخصصی، موقعیت کلی صنعت دفاعی در حوزه فناوری‌های سایبری، در ناحیه تدافعی-پویا تشخیص داده شد.

این تشخیص به‌معنای آن است که صنعت دفاعی، در شرایطی قرار دارد که نقاط ضعف داخلی بر نقاط قوت غلبه دارند و هم‌زمان، تهدیدات خارجی بر فرصت‌ها پیشی گرفته‌اند. با این حال، واژه «پویا» در این عنوان، نشان‌دهنده آن است که این موقعیت، یک موقعیت «مقدر و تغییرناپذیر» نیست؛ بلکه با اتخاذ راهبردهای مناسب، امکان گذار به نواحی مطلوب‌تر (رقابتی و حتی تهاجمی) نیز وجود دارد.



شکل ۱. موقعیت کلی در ناحیه تدافعی پویا.

مهم‌ترین نقاط قوت شناسایی‌شده، که خبرگان بر آنها اتفاق نظر داشتند، عبارتند از:

- سرمایه‌های انسانی جوان و نخبه که با وجود محدودیت‌های کمی، از نظر کیفی و انگیزشی، یک مزیت راهبردی محسوب می‌شوند.
- افزایش دقت و کاهش خطا که نتیجه مستقیم ورود فناوری‌های سایبری به فرایندهای تولید و عملیات است و در نمونه‌های موفقی همچون سامانه‌های پهپادی و موشکی به اثبات رسیده است.
- توان علمی در توسعه محصولات نرم‌افزاری دفاعی که نشان‌دهنده ظرفیت بالای داخل کشور در حوزه‌هایی مانند رمزنگاری، شبیه‌سازی و سامانه‌های فرماندهی است.

[۱۲] CPS

[Downloaded from ic4i-journal.ir on 2026-11-21]

- سیاست‌های حمایتی فرماندهی معظم کل قوا و مسئولین ارشد کشور که بستر مناسبی برای سرمایه‌گذاری در حوزه‌های راهبردی فراهم کرده است.

در مقابل، بحرانی‌ترین نقاط ضعف که نیازمند توجه فوری بودند، از دیدگاه خبرگان عبارت بودند از:

- کمبود نیروی انسانی متخصص و ماهر در حوزه‌های پیشرفته سایبری مانند کوانتوم، هوش مصنوعی و امنیت سایبری. این نقطه ضعف، با بالاترین میزان توافق (۹۶٪) به‌عنوان گلوگاه اصلی توسعه شناسایی شد.
- وابستگی به تجهیزات و فناوری‌های خارجی و آسیب‌پذیری‌های امنیتی ناشی از آن، که نه‌تنها هزینه‌های توسعه را افزایش می‌دهد، بلکه زنجیره تأمین را در برابر خرابکاری و نفوذ دشمن آسیب‌پذیر می‌کند.
- چالش‌های اقتصادی ناشی از تحریم و کمبود بودجه که برنامه‌ریزی بلندمدت را با مشکلات جدی مواجه می‌سازد و انگیزه سرمایه‌گذاری در پروژه‌های پرمخاطره را کاهش می‌دهد.
- عدم هماهنگی و یکپارچگی در سیاست‌گذاری‌های بین بخشی و موازی‌کاری که باعث هدررفت منابع و کندشدن روند توسعه فناوری می‌شود.

در زمینه فرصت‌های محیطی، خبرگان بر سه مورد زیر تأکید داشتند:

- افزایش اهمیت امنیت سایبری در سطح بین‌المللی و گستردگی کاربرد فناوری‌های سایبری در حوزه‌های مختلف نبرد، که بازار بالقوه بزرگی برای محصولات داخلی ایجاد کرده است.
- نیازمندی بالای نیروهای مسلح به محصولات مبتنی بر فناوری‌های سایبری، که به‌عنوان یک «مشتری آماده و مشتاق» می‌تواند محرک اصلی توسعه باشد.
- بهره‌گیری از ظرفیت شرکت‌های فناور و دانش‌بنیان و پارک‌های علم‌وفناوری که در سال‌های اخیر، رشد قابل‌توجهی داشته و می‌توانند به‌عنوان بازوهای اجرایی توسعه فناوری عمل کنند.

در نهایت، جدی‌ترین تهدیدهایی که پیش روی صنعت دفاعی قرار دارند، عبارتند از:

- مهاجرت نخبگان که سرمایه‌های انسانی کلیدی کشور را به سمت کشورهای رقیب سوق می‌دهد.
- تحریم‌ها و محدودیت‌های بین‌المللی در دسترسی به لبه‌های فناوری و تجهیزات پیشرفته، که مسیر بومی‌سازی را طولانی و پرهزینه می‌سازد.
- رشد و توسعه سریع فناوری در کشورهای پیشرو و خطر جاماندگی از رقبای جهانی، که در صورت بی‌توجهی، شکاف فناورانه را به‌سرعت افزایش خواهد داد.
- افزایش تهدیدات سایبری پیچیده در زیرساخت‌ها و ارائه سلاح‌های سایبرپایه از سوی دشمنان، که ضرورت مصون‌سازی را بیش از پیش آشکار می‌سازد.

۳.٤. راهبردهای کلان (٤ محور مفهومی)

بر اساس تحلیل موقعیت تدافعی-پویا، راهبردهای کلان در چهار محور مفهومی تدوین شدند که هر یک، پاسخی نظام‌مند به یکی از چالش‌های اساسی شناسایی‌شده هستند. این محورها، به‌عنوان «جهت‌گیری‌های اصلی» صنعت دفاعی در افق ۱۰ ساله، به‌کار گرفته خواهند شد:

محور اول: بازآفرینی نهادی و حکمرانی یکپارچه

این محور، پاسخی به نقطه ضعف «عدم هماهنگی و یکپارچگی در سیاست‌گذاری‌های بین‌بخشی» و «موازی‌کاری» است. راهبرد کلان در این محور، طراحی و استقرار یک نظام حکمرانی یکپارچه در سطح کلان صنعت دفاعی با هدف یکپارچه‌سازی سامانه‌های فرماندهی و کنترل و ارتقای هماهنگی بین‌نیرویی در چرخه تصمیم‌گیری که شامل چهار اقدام اساسی می‌شود: ایجاد «شورای عالی راهبردی فناوری‌های سایبری دفاعی» به‌عنوان نهاد فرابخشی با حضور نمایندگان وزارت دفاع، ستاد کل نیروهای مسلح، وزارت علوم، معاونت علمی ریاست‌جمهوری و صنایع دفاعی کلیدی؛ استقرار «نظام مدیریت یکپارچه پروژه‌های فناوری سایبری» از طریق طراحی و پیاده‌سازی سکوی ملی اشتراک دانش و اطلاعات پروژه‌ها؛ و اصلاح فرایندهای ارزیابی

[Downloaded from ic4i-journal.ir on 2026-11-21]

و تأمین مالی پروژه‌ها با رویکرد «چابکی» و «پذیرش مخاطره حساب‌شده»

محور دوم: خوداتکایی فناورانه و بومی‌سازی هوشمند

این محور، پاسخ مستقیمی به نقاط ضعف «وابستگی به فناوری خارجی»، «چالش‌های تحریم» و تهدید «قطع دسترسی به لبه‌های فناوری» است. راهبرد کلان در این محور، عبور از «بومی‌سازی تقلیدی» به «خوداتکایی هوشمند» است؛ به‌این‌معنا که بومی‌سازی نباید صرفاً به معنای کپی‌برداری از محصولات خارجی باشد، بلکه باید به‌عنوان فرصتی برای خلاقیت و دستیابی به راه‌حل‌های نوآورانه و متناسب با نیازهای بومی تلقی شود. اقدامات اساسی این محور عبارتند از: ۱- ایجاد «مراکز ملی پیشران» در حوزه‌های سه‌گانه «فناوری کوانتوم و رمزنگاری پساکوانتومی»، «هوش مصنوعی دفاعی» و «امنیت سایبری» با مشارکت صنعت، دانشگاه و نیروهای مسلح؛ ۲- طراحی و اجرای برنامه ملی «بومی‌سازی اقلام راهبردی و حیاتی» در زنجیره تأمین فناوری‌های سایبری با اولویت‌بندی شفاف و ضرب‌الاجل‌های معین؛ ۳- ایجاد زیرساخت ملی شبیه‌سازی و آزمون فناوری‌های سایبری با عنوان «میدان تمرین سایبری ملی» که امکان آزمون و ارزیابی محصولات دفاعی سایبری را در محیطی امن و واقع‌گرایانه فراهم می‌کند و ٤- طراحی و پیاده‌سازی سامانه یکپارچه **ISR٤C** مبتنی بر معماری باز و مدولار با قابلیت اتصال به تمامی سامانه‌های تسلیحاتی و حسگرهای میدان نبرد و کاهش زمان چرخه تصمیم‌گیری

محور سوم: توانمندسازی سرمایه انسانی و جلوگیری از فرار مغزها

این محور، پاسخی به بحرانی‌ترین نقطه ضعف (کمبود نیروی متخصص) و مهم‌ترین تهدید (مهاجرت نخبگان) است. راهبرد کلان در این محور، تبدیل «تهدید مهاجرت» به «فرصت شبکه‌سازی جهانی» و درعین‌حال، ایجاد انگیزه‌های قوی برای ماندگاری نخبگان در داخل کشور است. اقدامات اساسی عبارتند از: طراحی و اجرای برنامه ملی «پایوران متخصص فناوری‌های سایبری دفاعی» با بازنگری در سرفصل‌های آموزشی و هدف‌گذاری برای تربیت هزاران متخصص طی ۵ سال؛ ایجاد «بسته‌های تشویقی جذاب و متنوع» (مالی، رفاهی، شغلی و پژوهشی) برای نخبگان؛ و راه‌اندازی «دروازه علم‌وفناوری» برای جذب و به‌کارگیری نخبگان ایرانی خارج از کشور از طریق برنامه‌های همکاری موقت.

محور چهارم: تاب‌آوری اقتصادی و تأمین مالی پایدار

این محور، پاسخ به نقاط ضعف «چالش‌های اقتصادی ناشی از تحریم و کمبود بودجه» است. راهبرد کلان در این محور، طراحی یک «سیستم مالی مقاوم و خلاق» است که بتواند پروژه‌های بلندمدت و پرمخاطره فناوری‌های سایبری را تأمین مالی کند. اقدامات اساسی عبارتند از: ایجاد «صندوق سرمایه‌گذاری خطرپذیر تخصصی فناوری‌های سایبری دفاعی» با مشارکت صنایع دفاعی بزرگ، بانک‌های دولتی و معاونت علمی ریاست‌جمهوری؛ طراحی الگوی تأمین مالی ترکیبی (دولتی-خصوصی) با استفاده از ابزارهایی همچون «اوراق مشارکت فناوری» و «قراردادهای مرحله‌ای»؛ و توسعه بازارهای صادراتی محصولات دفاعی سایبری به کشورهای همسو از طریق دیپلماسی دفاعی.

جدول ۲ جزئیات این راهبردها و اقدامات اساسی مرتبط با هر یک را به‌صورت شفاف نشان می‌دهد.

جدول ۲. راهبردهای کلان در چهار محور مفهومی و اقدامات اساسی.

محور راهبردی	راهبرد کلان	اقدامات اساسی (با قابلیت اندازه‌گیری)
بازآفرینی نهادی	استقرار نظام حکمرانی یکپارچه برای رفع موازی‌کاری	۱. ایجاد شورای عالی راهبردی (طی ٦ ماه) ۲. استقرار سکوی ملی اشتراک دانش پروژه‌ها ۳. اصلاح فرایندهای ارزیابی با رویکرد چابکی
خود اتکایی فناورانه	عبور از بومی‌سازی تقلیدی به خوداتکایی هوشمند	۱. ایجاد ۳ مرکز ملی پیشران (کوانتوم، هوش مصنوعی، امنیت سایبری) ۲. تدوین نقشه راه بومی‌سازی اقلام حیاتی (تا ۳ سال) ۳. راه‌اندازی میدان تمرین سایبری ملی
توانمند سازی سرمایه انسانی	تبدیل تهدید مهاجرت به فرصت شبکه‌سازی جهانی	۱. .برنامه ملی «پایوران متخصص» (تربیت ۱۰۰۰ متخصص در ۵ سال) ۲. طراحی بسته‌های تشویقی جذاب و متنوع

[Downloaded from ic4i-journal.ir on 2026-11-21]

		۳. راه‌اندازی «دروازه علم‌وفناوری» برای نخبگان خارج از کشور
تاب‌آوری اقتصادی	طراحی سیستم مالی مقاوم و خلاق برای تأمین مالی پایدار	۱. ایجاد صندوق سرمایه‌گذاری خطرپذیر تخصصی ۲. طراحی الگوی تأمین مالی ترکیبی (دولتی-خصوصی) ۳. توسعه بازارهای صادراتی با دیپلماسی دفاعی

٤.٤. راهبردهای عملیاتی (۷ خوشه معنایی)

راهبردهای عملیاتی که تعداد آنها به ۸۰ می‌رسد، به‌منظور تسهیل فهم و اجرا، در هفت خوشه معنایی دسته‌بندی شده‌اند. این خوشه‌ها، درواقع «پل ارتباطی» میان راهبردهای کلان (که در سطح صنعت و درون‌سازمانی مطرح هستند) و فناوری‌های ده‌گانه در عرصه‌های پنج‌گانه نبرد محسوب می‌شوند. هر خوشه، نماینده یک «حوزه کارکردی» است که در آن، ترکیبی از چند فناوری، در خدمت هدفی مشخص قرار می‌گیرند. این رویکرد، از پراکندگی و بخشی‌نگری جلوگیری کرده و هم‌افزایی میان فناوری‌ها را تسهیل می‌کند.

خوشه اول: تصمیم‌یارهای هوشمند (مبتنی بر هوش مصنوعی و کلان‌داده)

شامل توسعه سامانه‌های پیش‌بینی تهدید با استفاده از یادگیری عمیق، طراحی سامانه‌های هماهنگ‌کننده عملیات در عرصه‌های پنج‌گانه، پیاده‌سازی الگوریتم‌های تحلیل خودکار داده‌های میدان نبرد، و سرمایه‌گذاری هدفمند در آموزش و جذب نیروی متخصص هوش مصنوعی.

خوشه دوم: امنیت ارتباطات و رمزنگاری (مبتنی بر کوانتوم، بلاک‌چین و رمزنگاری پساکوانتومی)

شامل توسعه زیرساخت توزیع کلید کوانتومی[۱۳] برای شبکه‌های فرماندهی و کنترل حساس، طراحی و پیاده‌سازی رمزنگاری پسا کوانتوم[۱۴] برای سامانه‌های موجود، ایجاد شبکه‌های ارتباطی مقاوم در برابر نفوذ با استفاده از بلاک‌چین، و تدوین استانداردهای ملی برای استفاده عملیاتی از فناوری کوانتوم.

خوشه سوم: سامانه‌های خودمختار و رباتیک (مبتنی بر سامانه‌های خودمختار، اینترنت اشیا و **CPS**)

شامل توسعه پهپادهای انتحاری خودمختار با قابلیت تشخیص و حمله مستقل به اهداف، طراحی سامانه‌های خودمختار شناسایی و نجات، پیاده‌سازی سامانه سوخت‌رسانی هوایی خود مختاروعملیات گروهی پهپادها، و سرمایه‌گذاری در تحقیقات هماهنگی انسان-ماشین.

خوشه چهارم: پایش و شناسایی پیشرفته (مبتنی بر سنجش مجتمع و سایبر، اینترنت اشیا و حسگرهای هوشمند)

شامل توسعه شبکه‌های حسگر هوشمند برای نظارت بلادرنگ بر میدان نبرد، طراحی سامانه‌های هشدار سریع مبتنی بر حسگرهای چندمنظوره، ایجاد سامانه‌های یکپارچه شناسایی با ترکیب داده‌های راداری، فروسرخ، صوتی و لرزه‌ای، و سرمایه‌گذاری در تولید حسگرهای پیشرفته بومی.

خوشه پنجم: حاکمیت داده و استانداردسازی (مبتنی بر کلان‌داده، بلاک‌چین و معماری ابری)

شامل تدوین پروتکل‌های استاندارد مدیریت داده‌های نظامی، طراحی و پیاده‌سازی سامانه‌های یکپارچه جمع‌آوری و تحلیل داده‌های اطلاعاتی، ایجاد سامانه‌های مدیریت زنجیره تأمین شفاف با بلاک‌چین، و تدوین استانداردهای امنیت سایبری برای محصولات دفاعی.

خوشه ششم: آموزش و توانمندسازی نیروی انسانی (مبتنی بر رابط کاربری انسان-ماشین، واقعیت مجازی و شبیه‌سازی)

شامل طراحی و توسعه سامانه‌های آموزشی واقعیت مجازی و افزوده، تدوین دوره‌های آموزشی استاندارد و شبیه‌سازهای تعاملی، طراحی رابط‌های کاربری هوشمند و چندحسی برای سامانه‌های فرماندهی و کنترل، و برگزاری رزمایش‌های سالانه شبیه‌سازی حملات سایبری.

خوشه هفتم: یکپارچه‌سازی فرماندهی و کنترل و تسریع تصمیم‌گیری (مبتنی بر تمامی فناوری‌ها)، طراحی و پیاده‌سازی

[۱۳] QKD

[۱۴] PQC

[Downloaded from ic4i-journal.ir on 2026-11-21]

سامانه‌های یکپارچه فرماندهی و کنترل با قابلیت اتصال به تمامی عرصه‌های نبرد، ایجاد داشبوردهای راهبردی و عملیاتی برای فرماندهان با قابلیت نمایش بلادرنگ آگاهی وضعیتی، توسعه سامانه‌های پشتیبانی از تصمیم‌گیری فرماندهان با استفاده از هوش مصنوعی و کلان‌داده ، استقرار معماری **ISR٤C** یکپارچه در سطح نیروهای مسلح با تأکید بر کاهش زمان چرخه تصمیم‌گیری، طراحی سامانه‌های شبیه‌سازی و تمرین فرماندهی و کنترل در سناریوهای پیچیده سایبری

۵.٤. راهبردهای عملیاتی (۷ خوشه معنایی)

۸۰ راهبرد عملیاتی در هفت خوشه تدوین شده است که بصورت زیر خلاصه می‌شوند:

خوشه	فناوری‌های پایه	شرح مختصر
تصمیم‌یارهای هوشمند	هوش مصنوعی، کلان‌داده	توسعه سامانه‌های پیش‌بینی تهدید، هماهنگ‌کننده عملیات، تحلیل خودکار داده‌ها
امنیت ارتباطات	کوانتوم، بلاکچین	توسعه QKD ، پیاده‌سازی PQC ، شبکه‌های مقاوم با بلاکچین
سامانه‌های خودمختار	خودمختار، IoT، CPS	پهپادهای انتحاری، شناسایی و نجات، عملیات گروهی، هماهنگی انسان–ماشین
پایش و شناسایی پیشرفته	سنجش مجتمع، IoT	شبکه‌های حسگر هوشمند، هشدار سریع، شناسایی یکپارچه
حاکمیت داده	کلان‌داده، بلاکچین	استانداردسازی داده، مدیریت زنجیره تأمین شفاف، امنیت سایبری محصولات
آموزش و توانمندسازی	HMI، واقعیت مجازی	شبیه‌سازهای تعاملی، رابط‌های کاربری هوشمند، رزمایش‌های سایبری
یکپارچه‌سازی C۲	تمامی فناوری‌ها	سامانه یکپارچه C۲ ، داشبورد راهبردی، معماری C٤ISR ، کاهش زمان OODA

٦.٤. راهکارهای اساسی (در ٤ حوزه اجرایی)

برای تحقق راهبردهای کلان و عملیاتی، یک مجموعه از راهکارهای اساسی تدوین شده است که به‌عنوان «اقدامات عینی و زمان‌بندی‌شده» قابل اجرا هستند. این راهکارها در چهار حوزه مجزا دسته‌بندی شده‌اند تا مدیریت و پیگیری آنها تسهیل شود:

حوزه نهادی و حاکمیتی:

- تشکیل کارگروه‌های حل مسئله با حضور نمایندگان دستگاه‌های مرتبط برای رفع گلوگاه‌های فرابخشی و تسریع در تصمیم‌گیری‌های کلان.
- بازنگری در آیین‌نامه‌های تدارکات دفاعی به‌منظور تسریع فرایندهای تحقیق و توسعه و خرید نمونه‌های اولیه.
- تدوین منشور حقوق مالکیت فکری در پروژه‌های مشترک صنعت–دانشگاه به منظور تشویق همکاری‌های پژوهشی و جلوگیری از سرقت دانش.
- اصلاح فرایندهای ارزیابی و نظارت بر پروژه‌ها با رویکرد «پذیرش مخاطره حساب‌شده» و «آموزش از شکست‌ها» به‌جای رویکرد تنبیه‌محور صرف.

حوزه منابع انسانی:

- بازطراحی سرفصل‌های آموزشی دانشگاه‌های نظامی و مراکز علمی–کاربردی با محوریت هوش مصنوعی، کوانتوم، امنیت سایبری و تحلیل داده.
- ایجاد «مسیر شتاب‌دهنده نخبگان» برای ورود سریع استعدادهای برتر به پروژه‌های کلان فناوری سایبری با حذف تشریفات زائد اداری.
- طراحی و اجرای برنامه‌های تبادل استاد و دانشجو با دانشگاه‌های معتبر در کشورهای همسو (از مسیرهای رسمی و غیررسمی) برای به‌روز نگه‌داشتن دانش نیروهای متخصص.
- نهادینه‌سازی فرهنگ «یادگیری مستمر» و «به‌اشتراک‌گذاری دانش» در سازمان‌های دفاعی از طریق ایجاد انجمن‌های علمی تخصصی و انتشار نشریات داخلی.

حوزه فناوری و زیرساخت:

- راه‌اندازی «میدان تمرین سایبری ملی» با قابلیت شبیه‌سازی هم‌زمان پنج عرصه نبرد و سناریوهای پیچیده حملات سایبری، برای آزمون محصولات و آموزش تیم‌های واکنش سریع.

[Downloaded from ic4i-journal.ir on 2026-11-21]

- طراحی و پیاده‌سازی «سکوی ملی اشتراک دانش پروژه‌های فناوری سایبری» (با رعایت سطوح محرمانگی) به منظور ثبت تجارب، جلوگیری از دوباره‌کاری و تسهیل انتقال فناوری بین سازمانی.
- ایجاد «آزمایشگاه‌های مرجع» برای آزمون امنیت و انطباق تجهیزات دفاعی با استانداردهای ملی و بین‌المللی.
- استقرار معماری «اعتماد صفر» در شبکه‌های فرماندهی و کنترل به‌عنوان یک اصل بنیادین در طراحی تمامی سامانه‌های جدید.
- طراحی و پیاده‌سازی معماری **ISR4C** یکپارچه با رویکرد خدمت‌گرا و قابلیت اتصال به تمامی سامانه‌های تسلیحاتی مبتنی بر فناوری‌های سایبری

حوزه تأمین مالی و اقتصاد مقاومتی:

- تخصیص حداقل ۵ درصد از بودجه کل دفاعی به تحقیق و توسعه فناوری‌های سایبری به‌صورت مستقل و با نظارت شورای عالی راهبردی.
- طراحی نظام «قراردادهای مرحله‌ای» برای پروژه‌های پرمخاطره فناوری سایبری که در آن، پرداخت بودجه منوط به تحقق اهداف میان‌مرحله‌ای تعیین‌شده است.
- حمایت از صادرات محصولات سایبری دفاعی از طریق ارائه تسهیلات اعتباری، بیمه نامه‌های صادراتی و کمک به اخذ استانداردهای بین‌المللی برای کشورهای همسو.
- ایجاد «صندوق پژوهش و فناوری دفاعی» با مشارکت بخش خصوصی و شرکت‌های دانش‌بنیان برای تأمین مالی طرح‌های نوآورانه با پتانسیل تجاری‌سازی بالا.

جدول ۳ نمونه‌هایی از این راهکارها را در چهار حوزه اجرایی نشان می‌دهد.

جدول ۳. نمونه‌هایی از راهکارهای اساسی در حوزه‌های اجرایی.

حوزه اجرایی	نمونه راهکار اساسی	هدف
نهادی و حاکمیتی	بازنگری در آیین‌نامه‌های تدارکات دفاعی	تسریع فرایندهای تحقیق و توسعه و خرید نمونه‌های اولیه.
منابع انسانی	ایجاد مسیر شتاب‌دهنده نخبگان	ورود سریع استعدادهای برتر به پروژه‌های کلان با حذف تشریفات زائد.
فناوری و زیرساخت	راه‌اندازی میدان تمرین سایبری ملی	آزمون محصولات و آموزش تیم‌های واکنش سریع در محیطی امن و واقعی.
تأمین مالی	طراحی نظام قراردادهای مرحله‌ای	مدیریت ریسک پروژه‌های پرمخاطره با پرداخت بودجه مبتنی بر تحقق اهداف میان‌مرحله‌ای.

۵. طراحی الگوی نظارت و شاخص‌های جهت‌دهنده

اجرای موفق چارچوب راهبردی پیشنهادی، بدون استقرار یک نظام پایش و ارزیابی اثربخش، ممکن نیست. در این پژوهش، به‌جای طراحی شاخص‌های صرفاً کمی (که در عمل، به‌دلیل پیچیدگی و تغییرات مداوم، کارایی خود را از دست می‌دهند)، بر «شاخص‌های جهت‌دهنده» تأکید شده است. این شاخص‌ها، وضعیت را به‌صورت «نسبی و روندی» نشان می‌دهند و به مدیران امکان می‌دهند تا جهت‌گیری کلی را ارزیابی کنند، نه اینکه صرفاً درگیر اعداد دقیق و غیرقابل‌حصول شوند.

۱.۵. الگوی نظارت سه‌سطحی

الگوی نظارت پیشنهادی، دارای سه سطح است که هر یک، مخاطبان و اهداف مشخصی دارند:

سطح اول: نظارت درون‌سازمانی (پروژه‌محور)

این سطح توسط خود سازمان‌های مجری پروژه‌های فناوری سایبری انجام می‌شود و هدف آن، پایش پیشرفت روزانه و هفتگی پروژه‌هاست. شاخص‌های این سطح شامل مواردی چون «درجه هم‌راستایی پروژه با مضمون فراگیر» (آیا پروژه به ارتقای هوشمندی، امنیت یا یکپارچگی چرخه فرماندهی و کنترل کمک می‌کند؟)، «سرعت تصمیم‌گیری در شرایط پیش‌بینی‌نشده»، «نرخ جذب و نگهداشت نیروی متخصص در پروژه» و « بهبود حلقه تصمیم‌گیری (زمان چرخش حلقه مشاهده-جهت‌گیری-تصمیم-اقدام) » هستند. گزارش‌های این سطح، به‌صورت ماهانه به سطح دوم ارسال می‌شوند.

سطح دوم: نظارت فرابخشی (هماهنگ‌کننده)

[Downloaded from ic4i-journal.ir on 2026-11-21]

این سطح توسط «شورای عالی راهبردی فناوری‌های سایبری دفاعی» انجام می‌شود و هدف آن، پایش هماهنگی بین دستگاه‌ها و تخصیص بهینه منابع در سطح کلان است. شاخص‌های کلیدی این سطح عبارتند از: «نرخ هم‌افزایی بین سازمانی» (که نشان‌دهنده کاهش موازی‌کاری و افزایش اشتراک‌گذاری است)، «شاخص مهاجرت معکوس نخبگان» به صنعت دفاعی و «نرخ تحقق اهداف میان‌مدت نقشه‌راه ملی». نرخ یکپارچگی سامانه‌های فرماندهی کنترل (درجه اتصال و هماهنگی بین سامانه‌های فرماندهی). جلسات این شورا، هر سه ماه یکبار برگزار و گزارش‌های تحلیلی به سطح سوم ارائه می‌شود.

سطح سوم: نظارت راهبردی (بالادستی)

این سطح توسط مقام عالی وزارت دفاع (یا ستاد کل نیروهای مسلح) انجام می‌شود و هدف آن، ارزیابی تأثیر کلی چارچوب بر امنیت ملی و توان دفاعی کشور است. شاخص‌های راهبردی این سطح عبارتند از: «تاب‌آوری کل صنعت دفاعی» در برابر حملات سایبری فراگیر (که با استفاده از شبیه‌سازی‌های دوره‌ای اندازه‌گیری می‌شود)، «نرخ خوداتکایی در فناوری‌های حیاتی»، «نرخ صادرات محصولات دفاعی سایبری» و « شاخص بلوغ یا سطح آمادگی و یکپارچگی سامانه‌های فرماندهی، کنترل» به‌عنوان شاخصی از توان رقابتی. این سطح، سالانه دو بار تشکیل جلسه داده و در صورت نیاز، دستور بازنگری در راهبردهای کلان را صادر می‌کند.

۲.۵. حلقه‌های بازخورد مفهومی

ویژگی کلیدی این الگوی نظارت، وجود سه حلقه بازخورد است که چارچوب را از یک مدل ایستا به یک «سازمان یادگیرنده پویا» تبدیل می‌کند:

حلقه اول (کوتاه‌مدت – ماهانه): نتایج سطح اول، مستقیماً به تیم‌های اجرایی بازخورد داده می‌شود تا اصلاحات سریع در مسیر اجرای پروژه انجام شود.

حلقه دوم (میان‌مدت – سالانه): نتایج سطح دوم، به‌عنوان ورودی برای بازنگری در برنامه‌های عملیاتی و تخصیص بودجه سال بعد استفاده می‌شود.

حلقه سوم (بلندمدت – هر ۳ سال): نتایج سطح سوم، به‌عنوان مبنایی برای بازنگری در راهبردهای کلان و حتی به‌روزرسانی مضمون فراگیر (در صورت تغییر پارادایم‌های جهانی) قرار می‌گیرد.

این مکانیزم بازخورد، تضمین می‌کند که چارچوب، همواره با تحولات سریع فناوری و تغییرات محیط امنیتی، هم‌گام و هم‌سو باقی بماند و به‌مرور زمان، کارایی خود را افزایش دهد، نه اینکه کاهش دهد.

برای پایش اثربخشی راهبردها، شاخص‌های جهت‌دهنده به‌جای صرفاً کمی بودن، وضعیت را به‌صورت نسبی و روندی نشان می‌دهند. رابطه (۲) نحوه محاسبه شاخص ترکیبی تاب‌آوری را به‌عنوان یک شاخص کلان نشان می‌دهد که می‌تواند در سطح سوم نظارت مورد استفاده قرار گیرد:

معادله (۲): محاسبه شاخص ترکیبی تاب‌آوری صنعت دفاعی

$$\text{Resilience_Index} = w_1 * (\text{Self_Sufficiency_Rate}) + w_2 * (\text{Incident_Recovery_Time}) + w_3 * (\text{Redundancy_Level})$$

که در آن w_1, w_2, w_3 وزن‌های اختصاص‌یافته به هر مؤلفه بر اساس اولویت‌های راهبردی هستند.

جدول ٤ شاخص‌های کلیدی هر سطح نظارتی را به همراه واحد اندازه‌گیری و بسامد ارزیابی نشان می‌دهد.

جدول ٤. شاخص‌های جهت‌دهنده در سطوح سه‌گانه نظارت.

سطح نظارت	شاخص‌های جهت‌دهنده کلیدی	واحد اندازه‌گیری / نحوه محاسبه	بسامد ارزیابی
سطح اول (درون‌سازمانی)	۱.درجه هم‌راستایی با مضمون فراگیر ۲.نرخ جذب و نگهداشت متخصص سرعت ۳.تصمیم‌گیری در شرایط پیش‌بینی‌نشده ٤.بهبود حلقه تصمیم‌گیری	۱. درصد (ارزیابی کیفی توسط گروه خبرگان) ۲. درصد (تعداد جذب‌شده / تعداد هدف) ۳. میانگین زمان (ساعت) از مواجهه تا تصمیم ٤. میانگین زمان (ثانیه/دقیقه) از تشخیص	ماهانه
سطح دوم (فرایخشی)	۱. نرخ هم‌افزایی بین سازمانی ۲. شاخص مهاجرت معکوس نخبگان ۳. نرخ تحقق اهداف میان‌مدت نقشه‌راه	۱.تعداد پروژه‌های اشتراکی / کل پروژه‌ها ۲. تعداد نخبگان بازگشته به صنعت دفاعی	فصلی

[Downloaded from ic4i-journal.ir on 2026-11-21]

	٤.درجه اتصال و هماهنگی بین سامانه‌های فرماندهی	٣. درصد پیشرفت فیزیکی پروژه‌های کلیدی ٤.درصد (تعداد سامانه‌های متصل / کل سامانه‌های فرماندهی)	
سطح سوم (راهبردی)	١. تاب‌آوری کل صنعت دفاعی ٢. نرخ خوداتکایی در فناوری‌های حیاتی ٣. نرخ صادرات محصولات دفاعی سایبری ٤. شاخص بلوغ یا سطح آمادگی و یکپارچگی سامانه‌های فرماندهی، کنترل	١. شاخص ترکیبی (از رابطه ٢) ٢. درصد (تعداد فناوری‌های بومی‌شده / کل فناوری‌های حیاتی) ٣. رصد رشد سالانه صادرات ٤. – واحد: بر اساس مدل بلوغ سازمانی	سالانه

ویژگی کلیدی این الگوی نظارت، وجود سه حلقه بازخورد است که چارچوب را از یک مدل ایستا به یک «سازمان یادگیرنده پویا» تبدیل می‌کند: حلقه اول (کوتاه‌مدت – ماهانه): نتایج سطح اول، مستقیماً به تیم‌های اجرایی بازخورد داده می‌شود تا اصلاحات سریع در مسیر اجرای پروژه انجام شود. حلقه دوم (میان‌مدت – سالانه): نتایج سطح دوم، به‌عنوان ورودی برای بازنگری در برنامه‌های عملیاتی و تخصیص بودجه سال بعد استفاده می‌شود. حلقه سوم (بلندمدت – هر ٣ سال): نتایج سطح سوم، به‌عنوان مبنایی برای بازنگری در راهبردهای کلان و حتی به‌روزرسانی مضمون فراگیر (در صورت تغییر پارادایم‌های جهانی) قرار می‌گیرد. این مکانیزم بازخورد، تضمین می‌کند که چارچوب، همواره با تحولات سریع فناوری و تغییرات محیط امنیتی، هم‌گام و هم‌سو باقی بماند و به‌مرور زمان، کارایی خود را افزایش دهد، نه اینکه کاهش دهد.

٦. بحث و تفسیر

چارچوب پیشنهادی در این پژوهش، در مقایسه با مدل‌های سنتی برنامه‌ریزی راهبردی که عمدتاً بر «تحلیل موقعیت» و «تدوین راهبردهای ایستا» تأکید دارند، از سه مزیت اساسی برخوردار است. نخست، انعطاف‌پذیری ذاتی که از طریق حلقه‌های بازخورد سه‌گانه محقق شده است. این ویژگی، به صنعت دفاعی اجازه می‌دهد تا بدون نیاز به طراحی مجدد کل چارچوب، مسیر خود را در مواجهه با تغییرات غیرمنتظره (مانند ظهور یک فناوری جدید یا تغییر در راهبرد دشمن) اصلاح کند. در دنیایی که پیشرفت فناوری‌های سایبری به‌صورت نمایی در حال رخداد است، این انعطاف‌پذیری، نه یک مزیت رقابتی، بلکه یک ضرورت بقا محسوب می‌شود.

دوم، شفافیت مفهومی یا همان «درک مشترک از چرایی و چگونگی اقدامات» است. با وجود مضمون فراگیر به‌عنوان «قطب‌نمای راهبردی»، تمامی ذی‌نفعان اعم از سیاست‌گذار، مجری و ارزیاب، درکی یکسان از هدف غایی دارند. این درک مشترک، از انحراف پروژه‌ها به سمت اهداف حاشیه‌ای یا کم‌اهمیت جلوگیری می‌کند و همچنین، ارتباط و هماهنگی بین بخش‌های مختلف را تسهیل می‌نماید. در بسیاری از سازمان‌های دفاعی، فقدان همین «زبان مشترک» باعث می‌شود که تلاش‌های گسترده، در نهایت به‌خاطر عدم هم‌راستایی، به نتیجه مطلوب نرسند.

سوم، پایداری در بلندمدت است. رویکرد حلقه‌بسته با نهادینه‌سازی «یادگیری سازمانی»، وابستگی به تصمیم‌گیری‌های سلیقه‌ای یا مقطعی را کاهش داده و یک «حافظه سازمانی» برای صنعت دفاعی ایجاد می‌کند. به‌عبارتی، تجارب موفق و ناموفق، ثبت، تحلیل و در بازنگری‌های بعدی لحاظ می‌شوند و این امر، از تکرار اشتباهات گذشته و هدررفت منابع جلوگیری می‌کند. این ویژگی، به‌ویژه در صنعت دفاعی که هزینه‌های خطا بسیار بالا است، از اهمیت ویژه‌ای برخوردار است.

در زمینه نحوه تحقق تسریع چرخه تصمیم‌گیری و حل پارادوکس توسعه و امنیت حاصل از توسعه و پشتیبانی از فناوری های سایبری در صنعت دفاعی می‌توان گفت، راهبردهای تدوین‌شده در این پژوهش، به‌طور مستقیم به تسریع چرخه تصمیم‌گیری (**OODA**) کمک می‌کنند. در مرحله مشاهده، توسعه شبکه‌های حسگر هوشمند و سامانه‌های سنجش مجتمع، سرعت و دقت جمع‌آوری داده‌ها را افزایش می‌دهند. در مرحله

[Downloaded from ic4i-journal.ir on 2026-11-21]

جهت‌گیری، سامانه‌های تصمیم‌یار هوشمند مبتنی بر هوش مصنوعی و کلان‌داده، تحلیل و تفسیر داده‌ها را تسریع می‌کنند. در مرحله تصمیم، داشبوردهای راهبردی یکپارچه و معماری **ISR4C**، آگاهی وضعیتی فرماندهان را ارتقا داده و تصمیم‌گیری را تسهیل می‌کنند. در مرحله اقدام، سامانه‌های خودمختار و ارتباطات امن کوانتومی، اجرای سریع و دقیق تصمیمات را ممکن می‌سازند. هم‌زمان، راهبردهای مصونیت‌بخشی (مانند رمزنگاری پساکوانتومی، معماری اعتمادصفر و استانداردهای امنیت سایبری) و راهبردهای توسعه، پارادوکس بنیادین را حل می‌کنند و امکان توسعه هم‌زمان با امنیت را فراهم می‌آورند. بنابراین، شکاف میان توسعه و امنیت با اتخاذ راهبردهای دوگانه (ارتقای قابلیت‌ها و مصونیت‌بخشی) پر می‌شود و تسریع چرخه **OODA** از طریق یکپارچه‌سازی فناوری‌ها در سامانه‌های **ISR4C** محقق می‌گردد.

مقایسه این چارچوب با تجارب موفق جهانی نیز نشان‌دهنده انطباق آن با رویکردهای نوین است. برای مثال، راهبرد علم‌وفناوری وزارت دفاع آمریکا (۲۰۲۳) نیز بر «سرعت، مقیاس و همکاری» تأکید دارد و به‌صراحت اشاره می‌کند که مدل‌های سنتی خطی، پاسخگوی چالش‌های عصر حاضر نیستند.

همچنین، برنامه‌های «نوآوری دفاعی» ناتو بر ایجاد شبکه‌های همکاری و بازخورد سریع بین صنعت، دانشگاه و نیروهای مسلح متمرکز است که با رویکرد «حکمرانی یکپارچه» در این پژوهش هم‌خوانی کامل دارد. با این تفاوت که چارچوب ارائه‌شده در این مقاله، با تأکید بر «بومی‌سازی هوشمند» و «اقتصاد مقاومتی»، برای کشوری مانند ایران که با محدودیت‌های تحریمی مواجه است، کارآمدی بیشتری دارد و می‌تواند به‌عنوان یک «الگوی منطقه‌ای» برای سایر کشورهای درحال‌توسعه نیز مورد توجه قرار گیرد.

۷. نتیجه‌گیری و پیشنهادات

طراحی چارچوب پویای توسعه فناوری‌های سایبری با هدف تسریع چرخه تصمیم‌گیری فرماندهی و کنترل در جنگ‌های شبکه‌محور، پاسخی نظام‌مند به مسئله «شکاف میان توسعه و امنیت» و «جزیره‌ای‌عمل کردن دستگاه‌های متولی» است. این چارچوب، با اتصال منطقی میان شش عنصر کلیدی (مضمون فراگیر، تحلیل محیطی، راهبردهای کلان، راهبردهای عملیاتی، راهکارهای اساسی و الگوی نظارت)، یک «چرخه حیات راهبردی» شکل داده است که ضمن تأکید بر هوشمندی و امنیت به‌عنوان اهداف غایی، قابلیت انطباق با تحولات شتاب‌زده فناوری و تغییرات محیط امنیتی را نیز دارد.

مهم‌ترین دستاورد این پژوهش را می‌توان در دو ویژگی «یکپارچگی» و «پویایی» آن خلاصه کرد. یکپارچگی، از طریق ایجاد زنجیره علّی-معلولی میان سطوح مختلف برنامه‌ریزی (از کلان‌ترین جهت‌گیری‌ها تا جزئی‌ترین اقدامات) محقق شده است و پویایی، از طریق استقرار سه حلقه بازخورد با افق‌های زمانی کوتاه‌مدت، میان‌مدت و بلندمدت تضمین شده است. این ویژگی‌ها، چارچوب را از یک سند صرفاً توصیفی یا تجویزی، به یک «ابزار مدیریت تحول» تبدیل می‌کند که می‌تواند به‌صورت عملی در صنعت دفاعی به‌کار گرفته شود.

بر اساس یافته‌های این پژوهش، پیشنهادات زیر برای سیاست‌گذاران و مدیران صنعت دفاعی ارائه می‌شود:

۱- تشکیل فوری «شورای عالی راهبردی فناوری‌های سایبری دفاعی»: این شورا باید با حضور نمایندگان وزارت دفاع، ستاد کل نیروهای مسلح، وزارت علوم، تحقیقات و فناوری، معاونت علمی و فناوری ریاست‌جمهوری و صنایع دفاعی کلیدی، هرچه سریع‌تر تشکیل شود. اولین وظیفه این شورا، تدوین «سند ملی فناوری‌های سایبری دفاعی» با افق ۱۰ ساله خواهد بود.

۲- آغاز برنامه‌ریزی برای راه‌اندازی «میدان تمرین سایبری ملی»: با توجه به ضرورت آزمون و ارزیابی محصولات دفاعی سایبری در محیطی امن و واقع‌گرایانه، طراحی و اجرای این پروژه زیرساختی باید در اولویت برنامه‌های ۳ ساله وزارت دفاع قرار گیرد. این میدان تمرین، می‌تواند نقشی مشابه «تارنمای ملی» برای حوزه سایبری دفاعی ایفا کند.

۳- طراحی و پیاده‌سازی «داشبورد راهبردی» بر اساس شاخص‌های جهت‌دهنده پیشنهادی: به‌منظور تسهیل نظارت و پایش مستمر، یک سامانه نرم‌افزاری یکپارچه طراحی شود که شاخص‌های سه سطح نظارتی را به‌صورت لحظه‌ای یا

[Downloaded from ic4i-journal.ir on 2026-11-21]

دوره‌ای نمایش دهد و هشدارهای لازم را در صورت انحراف از مسیر مورد انتظار، صادر نماید.

٤- بازنگری دوره‌ای چارچوب هر ۳ سال یکبار: با توجه به سرعت تغییرات فناوری، بازنگری در راهبردهای کلان و به‌روزرسانی نقشه‌راه ملی، هر ۳ سال یکبار با استفاده از مکانیزم حلقه بازخورد بلندمدت، انجام شود.

٥- بومی‌سازی شاخص‌ها و الگوی نظارت: با توجه به شرایط خاص کشور (تحریم‌ها، محدودیت‌های بودجه‌ای و ضرورت خوداتکایی)، شاخص‌های جهت‌دهنده پیشنهادی باید با مشارکت خبرگان صنعت دفاعی، بومی‌سازی و متناسب با نیازهای عملیاتی و اقتضائات فرهنگی-سازمانی، تعدیل شوند.

٦- طراحی و پیاده‌سازی یک سامانه یکپارچه فرماندهی و کنترل مبتنی بر هوش مصنوعی که بتواند داده‌های حاصل از تمامی فناوری‌های سایبری (هوش مصنوعی، کلان‌داده، اینترنت اشیا، سامانه‌های خودمختار، سنجش مجتمع و...) را در قالب یک داشبورد راهبردی به فرماندهان ارائه دهد و با تسریع چرخه تصمیم‌گیری، امکان تصمیم‌گیری سریع‌تر و دقیق‌تر را در شرایط بحرانی فراهم آورد.

در نهایت، این پژوهش نشان می‌دهد که صنعت دفاعی کشور، علی‌رغم چالش‌های متعدد، از ظرفیت‌های بالایی برای جهش در حوزه فناوری‌های سایبری برخوردار است. آنچه لازم است، «انتخاب راهبردهای صحیح» و «اجرای منسجم و پیگیرانه» آنهاست. چارچوب ارائه‌شده در این مقاله، می‌تواند به‌عنوان یک نقشه‌راه معتبر، مسیر این جهش را هموار سازد و زمینه‌ساز گذر از وضعیت فعلی (تدافعی-انفعالی) به وضعیت مطلوب (تهاجمی-فعالانه) در افق ١٤١٤ و فراتر از آن گردد.

۸. منابع

[١] J. W. Creswell and V. L. Plano Clark (٢٠١٧), "Designing and Conducting Mixed Methods Research", ٣rd ed. Thousand Oaks, CA, USA: SAGE Publications.

[٢] V. Braun and V. Clarke (٢٠٠٦), "Using thematic analysis in psychology," Qualitative Research in Psychology, vol. ٣, no. ٢, pp. ٧٧–١٠١.

[٣] F. R. David, Strategic Management (٢٠١١), Concepts and Cases, ١٣th ed. Upper Saddle River, NJ, USA: Prentice Hall.

[٤] K. Schwab (٢٠١٧), The Fourth Industrial Revolution. New York, NY, USA: Crown Business.

[٥] D. S. Alberts and R. E. Hayes (٢٠٠٣), Power to the Edge, Command and Control in the Information Age. Washington, DC, USA: CCRP Publication Series.

[٦] L. Kello (٢٠١٧), The Virtual Weapon and International Order. New Haven, CT, USA: Yale University Press.

[٧] L. Freedman (٢٠١٣), Strategy: A History. Oxford, UK: Oxford University Press.

[٨] M. E. O'Hanlon (٢٠٢٠), The Future of Land Warfare. Washington, DC, USA: Brookings Institution Press.

[٩] National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) Version ٢.٠, NIST CSWP ٢٩, Gaithersburg, MD, USA, ٢٠٢٤. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.٢٩.pdf

[١٠] U.S. Army, Multi-Domain Operations (TRADOC Pamphlet ٥٢٥-٣-١), Washington, DC, USA, ٢٠٢٢.

[١١] مهدی‌نژاد نوری، م. (١٤٠٠). نقش فناوری اطلاعات و ارتباطات در رشد صنعت دفاعی .فصلنامه دانش نظامی، ١٨(١)، ٩٠-٧٧.

[١٢] فولادی، م. (١٣٩٦). بررسی چالش‌های امنیتی در دنیای رقومی. فصلنامه امنیت ملی، ٧(٢٦)، ٣٨-١٥.

[١٣] ولوی، م.ر.، و مردانی شهربابک، م. (١٤٠٠). معماری سایبری نیروهای مسلح جمهوری اسلامی ایران با رویکرد دفاعی-امنیتی) سند اختصاصی شماره .(CAA١٠٩٠٤١ دانشگاه جامع امام حسین (ع).

[١٤] پژوهشکده امنیت دفاعی. (١٤٠٠). فناوری جدید و نوظهور شکل‌دهنده صحنه نبرد آینده (تک‌نگاشت دیده‌بان امنیت دفاعی شماره ٤٠). تهران.

[١٥] نیک نفس، ع. (١٣٩٩). الگوی بلوغ نظام رصد و پایش و هشداردهی سایبری جمهوری اسلامی ایران. رساله دکتری، دانشگاه عالی دفاع ملی، تهران.

[١٦] صمیمی، م.، حسینی، س.ح.، و اصغری، ح. (١٣٩٧). عوامل مؤثر بر نوآوری فناورانه در واحدهای صنعتی دفاعی. فصلنامه علوم و فناوری دفاعی، ١٢(٣)، ٦٨-٤٥.

[Downloaded from ic4i-journal.ir on 2026-11-21]

[۱۷] امیری، ح. (۱۳۹٦). طراحی الگوی پیش‌بینی فناوری‌های مؤثر دفاعی به منظور اجرای برنامه‌های راهبردی *مدیریت نظامی*، ۱۷(٦٥)، ۵۳-۲۹.

[۱۸] فرمایشات قائد عظیم الشان شهید(ره) در خصوص ضرورت توسعه فناوری‌های نوین دفاعی. (بیانات و تدابیر، ۱۳۹٦-۱٤۰٤).

[Downloaded from ic4i-journal.ir on 2026-11-21]