راهبردهای پدافند غیرعامل درحوزه‌ی فناوری

رضا محمدی‌نیا[1]

محمد شامحمدی[2]

تاریخ دریافت: ۱۳۹۳/۱۰/۲ **تاریخ پذیرش: ۱۳۹۴/۰۱/۲۸**

چکیده

این تحقیق که از نظر نوع هدف، کاربردی– توسعه‌ای و از نظر نوع گردآوری داده‌ها و پردازش اطلاعات، توصیفی و مطالعه‌ی موردی- زمینه‌ای است، با تلفیق دو حوزه‌ی پدافند غیرعامل و فن‌آوری، تلاش نموده راهبردهایی به منظور حفظ زیرساخت‌های فناوری کشور در سطح راهبردی ارائه نماید. برای تحقق چنین هدفی، با نشستی مشورتی با مسئولین سازمان پدافند غیرعامل کشور، بیست نفر از کسانی که در هر دو حوزه‌ی پدافند غیرعامل و فناوری صاحبنظر بوده‌اند به عنوان جامعه‌ی آماری همکاری داشته و متغیرهای تحقیق یعنی «پدافند غیرعامل» و «عناصر حوزه‌ی فناوری» مورد بررسی قرار گرفته و با تأکید بر بهره‌گیری از اصول و اقدامات پدافند غیرعامل، راهکارها و راهبردهایی با ماهیت تقویتی، توسعه‌ای، تولیدی، تحقیقاتی و تحکیمی به‌منظور ایمن‌سازی و پایدارسازی عناصر چهارگانه‌ی فناوری، یعنی «انسان، اطلاعات، ابزار و سازمان» به دست آمده است.

کلید واژه‌ها: پدافند غیرعامل. فن‌آوری. راهبرد.

۱- دکترای علوم دفاعی راهبردی و استادیار دانشگاه،

۲- نویسنده مسئول و دانشجوی دکترای علوم دفاعی راهبردی، mshamohammdy@yahoo.com

مقدمه

کشور جمهوری اسلامی ایران به‌دلیل برخورداری از نوع ایدئولوژی، آرمان‌ها و اهداف انقلاب اسلامی و نیز موقعیت خاص ژئوپلیتیک و ژئواستراتژیک در سطح منطقه و جهان، همواره در معرض تهدیدات مستمر و ناخواسته ای قرار داشته و دارد، و برابر قرائن و شواهد آشکار، اصلی ترین و عمده‌ترین تهدید مفروض(امام خامنه ای، ۱۳۷۵/۱۱/۱۲ و ۱۳۷۵/۸/۳۰) برای ایران، ایالات متحده آمریکا و هم‌پیمانان منطقه‌ای و بین‌المللی آن به ویژه رژیم صهیونیستی (امام خامنه‌ای، ۱۳۷۹/۵/۵) می‌باشند، لذا موضوع امنیت و دفاع در عرصه و مقیاس ملی، در مقابل چنین تهدیدی، در دستور کار دائمی و همیشگی ایران اسلامی قرار دارد.

ضمن اینکه تجربیات حاصل از جنگ تحمیلی و خسارت‌های وارده ناشی از تهاجم دشمن به تأسیسات و زیرساخت‌های نظامی، اقتصادی و صنعتی کشور و روحیه‌ی توسعه‌طلبی و سلطه‌گری نظام حاکم بر دولت‌مردان آمریکا (امام خامنه‌ای، ۱۳۷۴/۱۲/۱) در تهاجم مستقیم یا تحریک عوامل منطقه‌ای در ایجاد بحران‌های جدید، جدی و عمیق در مواجهه با جمهوری اسلامی ایران (امام خامنه‌ای ۱۳۶۸/۳/۱۹)، (به‌ویژه پس از اشغال عراق و افغانستان که بیش از هر زمان دیگری در همسایگی ایران و در منطقه‌ی خاورمیانه حضور یافته‌اند)، لزوم توجه به دفاع بهینه را که ترکیب و تلفیقی از پدافند عامل و غیرعامل می‌باشد و نیز ارائه‌ی راهبردهای مقابله‌ای لازم در حوزه‌های مختلف و از جمله حوزه‌ای فراگیر به نام فناوری را که موضوع این تحقیق می‌باشد را ایجاب می‌نماید.

فناوری به معنای عام آن یعنی «دانش فنی» یا «علم هنرهای صنعتی» یا استفاده از دانش علمی برای اهداف عملی، به‌ویژه در صنعت و در مفهوم اصطلاحی آن به عنوان پدیده‌ای که مجموعه‌ای از اقدامات مختلف مانند دانش فنی، شناخت مواد، مهارت‌ها، طراحی محصول، فرآیند ساخت و تولید، توسعه و کنترل محصول را در بر می‌گیرد، به‌عنوان یکی از منابع مزیت رقابتی[1] کشورهای مختلف و از جمله ایران محسوب می‌شود و همراه با رشد این پدیده (به خصوص در ابعاد اطلاعاتی و ارتباطی)، چهره‌ی جنگ‌های نظامی و غیرنظامی در دنیا تغییر کرده و انواع جدیدی از جنگ‌ها از جمله جنگ الکترونیکی (هینی[2]، ۱۹۹۷:۴) ، جنگ ایده‌ها (روسناو[3]، ۲۰۱۰:۱۱۳۱)،

1 - Competitive Advantage
2 -Haeni
3 -Rosenau

جنـگ مـاهواره‌ای(شـاو[1]، ۲۰۱۱:۲۱)، جنـگ اطلاعـاتی (مولانـدر۲[2]، ۱۹۹۶:۱۱) ، جنـگ اینترنتـی (گوداگنـو[3]، ۲۰۱۰:۴۴۷)، جنـگ مجـازی (اولمسـتد[4]، ۲۰۰۹:۱۶)، جنـگ رایانـه‌ای (روشـنباخ[5]، ۲۰۱۰:۲)، جنـگ روانـی (کـورنیش[6]، ۲۰۱۰:۱۰)، جنـگ رسـانه‌ای(شـویهبرو[7]، ۲۰۱۳:۲۵)، جنـگ رباتیک(ورک[8]، ۲۰۱۴:۲۸)، جنگ سایبری(سالبچ[9]، ۲۰۱۴:۷) و... پا به عرصه‌ی وجود گذاشته اسـت است و چنین واژگانی امروز به کرات در ادبیـات نظـامی، دفـاعی و امنیتـی جهـان مـورد بحـث و بررسی قرار می‌گیرند و همگی دلالت بر کاربرد روش‌های مختلفی از فناوری دارند.

عرصه، ابزار، ابعاد و حوزه‌های مختلف فن‌آوری، نیز همچون سایر حوزه‌ها، در بحران‌ها، تهدیدها، اقـدام‌هـای خصـمانه و جنـگ‌هـا، بـه‌شـدت هـم تاثیرگـذار و هـم تأثیرپـذیر اسـت. شـناخت آسیب‌پذیری‌های فن‌آوری و ارائـه‌ی راهبردهـای بهینـه، گـام نخسـت و شـاید مهمتـرین گـام در خنثی‌سازی اقدام‌های خصمانه‌ی دشمن باشد و از جمله راه‌های اصولی مقابله بـا تهدیـدهای ایـن حوزه، توجه خاص به پدافند غیرعامـل اسـت (امـام خامنـه‌ای، ۱۳۸۷/۱۰/۲۱)، نتـایج و تجربیـات حاصل از جنگ‌های اخیر در منطقه و سایر نقاط جهان نشان داده که عدم توجه به پدافند غیرعامل، تلفات و ضایعات جبران ناپذیری برجای خواهد گذاشت.

آسیب‌پذیربودن حوزه‌ی فن‌آوری کشور ایران (زاوی[10]، ۲۰۱۲:۴۱) در مقابل تهدیدهای مفروض از یک طرف، و عدم برقراری توازن میان گستره، حجـم و شـدت تهدیـدها در حـوزه‌ی فـن‌آوری و اقدامات دفاع عامل از طرف دیگـر، برخـورداری از راهبردهـایی بـا رویکـرد پدافنـد غیرعامـل بـه حوزه‌ی فـن‌آوری و عنـاصـر مـرتبـط با آن را، از طریق انجام تحقیقی علمی بیش از پیش آشـکار، ضروری و توجیه‌پذیر می‌نماید. ضمن این‌که اتخاذ یک سلسله تدابیر و اقدامات احتیاطی پیشگیرانه که مستلزم به کارگیری جنگ افزار نباشند، گویای اهمیت موضوع است، چرا کـه مـی‌توانـد از وارد شدن خسارات مالی یا تلفات انسانی در این حوزه‌ی ملیِ اثربخش و پر کاربرد جلوگیری نمایـد یـا

1 -Shaw
2 -Molander
3 -Guadagno
4 -Olemstead
5 -Raushenbakh
6 -Cornish
7 -Shaihebrew
8 -work
9 -Saalbach
10 -Zeevi

میزان خسارات، صدمات و تلفات را به حداقل ممکن کاهش دهد. بنابراین مسئله‌ی تحقیق تدوین راهبردهایی با موضوع پدافند غیرعامل در حوزه‌ی فناوری است.

این تحقیق تلاش دارد ضمن تقویت راهبردهای پدافند غیرعامل در حوزه‌ی فن‌آوری، به‌صورت علمی، باعث تجمیع، همگرایی و همسو شدن منابع و تلاش‌های ملی در راستای ایجاد امنیت پایدار در حوزه‌ی فن‌آوری گردد.

«هدف اصلی» این تحقیق؛ شناخت راهبرد پدافند غیرعامل در حوزه‌ی فناوری است، که دو «هدف فرعی» یعنی؛ شناخت فرصت‌ها و تهدیدهای پدافند غیرعامل کشور در حوزه‌ی فناوری و نیز شناخت نقاط قوت و ضعف پدافند غیرعامل کشور در حوزه‌ی فناوری، به تحقق آن کمک می‌کنند. همچنین «سؤال اصلی» تحقیق عبارت است از: راهبردهای پدافند غیرعامل کشور در حوزه‌ی فناوری چیست؟ که با پاسخ به دو «سؤال فرعی» یعنی؛ فرصت‌ها و تهدیدهای پدافند غیرعامل کشور در حوزه‌ی فناوری کدام است؟ و نقاط قوت و ضعف پدافند غیرعامل کشور در حوزه‌ی فناوری کدام است؟ به این مهم دست خواهیم یافت.

مبانی نظری

با بررسی‌های به عمل آمده از پژوهش‌های انجام شده پیرامون موضوعات نزدیک به تحقیق حاضر مشخص گردید پژوهشی خاص این موضوع، انجام نشده، هر چند برخی تحقیقات نیز تا حدودی با آن در ارتباط هستند، که عبارتند از:

۱- الگوی مدیریت راهبردی پدافند غیرعامل، امیر گروسی، به راهنمائی سید محمد حسین ابطحی، رساله دکتری، دانشگاه علامه طباطبائی، ۱۳۹۱. این تحقیق برای توسعه‌ی پایدار و مداوم پدافند غیرعامل در سطح ملی؛ تلفیق دو حوزه‌ی پدافند غیرعامل و برنامه‌ریزی راهبردی را ارائه می‌کند که امکان برنامه‌ریزی راهبردی و اقدام در آن چارچوب را دراختیار می‌گذارد.

۲- تدوین راهبرد پدافند غیرعامل در شرکت مجتمع گاز پارس جنوبی با تأکید بر حفظ منابع انسانی، به راهنمایی دکتر کاوه تیمورنژاد، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، ۱۳۹۰. در این تحقیق به ارائه‌ی دو سناریوی عمده در جهت کاهش آسیب‌پذیری پرداخته است: سناریوی اول در ارتباط با آسیب‌پذیری نیروی انسانی فعال در زمان جنگ،

ساختمان‌ها، تأسیسات و تجهیزات حساس و فعال و ارائه‌ی راهبردها و برنامه‌هایی برای کاهش آسیب‌پذیری‌ها می‌باشد و سناریوی دوم به کاهش آسیب‌پذیری بخش‌های حساس و غیرفعال در زمان جنگ پرداخته و راهبردها و برنامه‌هایی برای کاهش آسیب‌پذیری-های نیروی انسانی، ساختمان‌ها و تجهیزاتی که امکان انتقال آن‌ها به نقاط امن و دور از خطر وجود ندارد، ارائه شده است.

۳- تدوین راهبرد ملی پدافند غیرعامل، موضوعِ مطالعات گروهی دانشجویان دوره‌ی ۱۴ دفاع ملی، به استاد محوری، سردار دکتر غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور، دانشگاه عالی دفاع ملی، ۱۳۸۷. در این مطالعه، آسیب شناسی زیرساخت‌های کلیدی کشور در حوزه‌ی ارتباطات، انرژی، صنعت دفاعی، فن‌آوری و مدیریت مردم و ارائه‌ی راهبردهایی در هر حوزه پرداخته شده است.

۴- دومین همایش ملی پدافند غیرعامل در مرکز همایش‌های بین المللی صدا و سیما، مجری: سازمان پدافند غیرعامل کشور، ۱۳۹۲. در این نشست، شناخت فن‌آوری‌های روز اطلاعاتی و سایبری، توسعه با توجه به شناخت و آگاهی از انواع تهدیدها، مصون سازی و آمادگی برای دفاع و بازدارندگی و توجه به چالش‌های احتمالی و افزایش نگاه‌های علمی در حوزه‌ی پدافند غیرعامل، مورد بحث و بررسی قرار گرفته است.

بر این اساس در تحقیقات قبلی، راهبرد یا راهبردهایی که به طور خاص به عناصر چهارگانه‌ی فناوری به صورت مجزا و به شرح آن‌چه در این تحقیق آمده، پرداخته باشند مشاهده نمی‌شود، از این رو تحقیق حاضر در نوع خود می‌تواند گویای نگرشی جدید به حوزه‌ی فناوری و عناصر مرتبط با آن باشد.

متغیرهای تحقیق نیز عبارتند از:

متغیر مستقل: راهبرد پدافند غیرعامل

در تعریف رسمی پدافند غیرعامل چنین گفته شده: «پدافند غیرعامل به مجموعه اقدامات غیرمسلحانه‌ای اتلاق می‌شود که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد.» (سیاست‌های کلی نظام در بخش پدافند غیرعامل ۱۳۸۹/۱۱/۲۹)

متغیر وابسته: فن‌آوری

برای فن‌آوری به فراخور ماهیت، سطح، روند تاریخی و توسعه‌ای، حوزه‌ی مطالعه، نگرش محققین، اهداف تحقیق و ... تعاریف متفاوتی ارائه شده و هر کس از زاویه‌ای خاص به این موضوع پرداخته است و همین مسئله موجب ایجاد برداشت‌ها و قرائت‌های مختلفی از تعریف این واژه‌ی مهم که برخی از آن به عنوامن «ثروت ملل»[1] نام می‌برند (Gancia, 2008: 4)، شده است، لذا هر چند ارائه‌ی تعریفی جامع و مانع از فناوری، دشوار است، ولی تعریف برگزیده از فن‌آوری برای این تحقیق عبارت است از: تمام دانش، محصولات، فرآیندها، ابزارها، روش‌ها و سیستم‌هایی که در جهت خلق و ساخت کالاها و ارائه‌ی خدمات به کار گرفته می‌شوند. (خلیل، ۱۳۸۳: ۲۲)

همچنین در اطلس فناوری، از فناوری به‌عنوان عامل تبدیل کننده‌ی عوامل تولید به کالاها و خدمات یاد شده که از چهار عنصر و مؤلفه‌ی: ۱) سخت افزار ۲) افزار اطلاعاتی یا دانش فنی، ۳) توانایی‌های انسانیِ فناوری، ۴) سازماندهی و مدیریت فناوری، تشکیل شده است. (مجموعه مقالات، ۱۳۸۲: ۱۳۸).

بر این اساس فن‌آوری از چهار جزء اساسی (Streenhuis, 2006: 1081) و [1] (Govindaraju,2010) به شرح زیر تشکیل شده و در این تحقیق نیز تمرکز اصلی در تدوین راهبردها بر همین عناصر گذارده شده است:

۱- انسان افزار[2] (منابع انسانی فرهیخته و دارای دانش، مهارت، تجربه وخلاقیت)

۲- سخت افزار[3] (شامل وسائل، ماشین آلات، تجهیزات، کالا و محصول)

۳- نرم افزار[4] (شامل تمامی اطلاعات، مستندات، نظریه ها و طرح‌ها)

۴- مدیریت یا سازمان افزار[5] (شامل مهارت‌های مدیریتی، ساختار سازمانی منعطف، محیط مناسب جهت شکوفائی و اثر بخشیِ سه جزء دیگر).

1 - Wealth of Nations
2 - Human ware
3 - Hardware
4 - Software
5 - Orgaware

چارچوب نظری و مدل مفهومی

در مبحث چارچوب نظری و مدل مفهومی تحقیق نیز به دو موضوع کلان یعنی «پدافند غیرعامل» و «فن‌آوری» و عناصر و محورهای اساسی مربوط به هر یک، اشاره شده است و همانطور که گفته شد پدافند غیرعامل به مجموعه‌ای از اصول، اقدامات، تدابیر و طرح‌هایی گفته می‌شود که رعایت به‌موقع و مناسب آن‌ها، محورهای اساسی پنجگانه‌ی پدافند غیرعامل را محقق می‌سازند و فن‌آوری نیز با توجه به مطالعه‌ی تاریخچه و مفاهیم مرتبط با آن در ایران و جهان، در این مقاله از جنس «توانایی» و دارای چهار جزء اصلی یعنی «انسان، اطلاعات، ابزار و سازمان» می‌باشد. این مقاله با بهره‌گیری از اصول پدافند غیرعامل در ارتباط با (عناصر چهارگانه‌ی) فناوری، به ارائه‌ی راهبردهایی پیرامون ایمن‌سازی و پایدارسازیِ این حوزه در برابر اقدامات سخت (نظامی/ جنگ) دشمن پرداخته است.

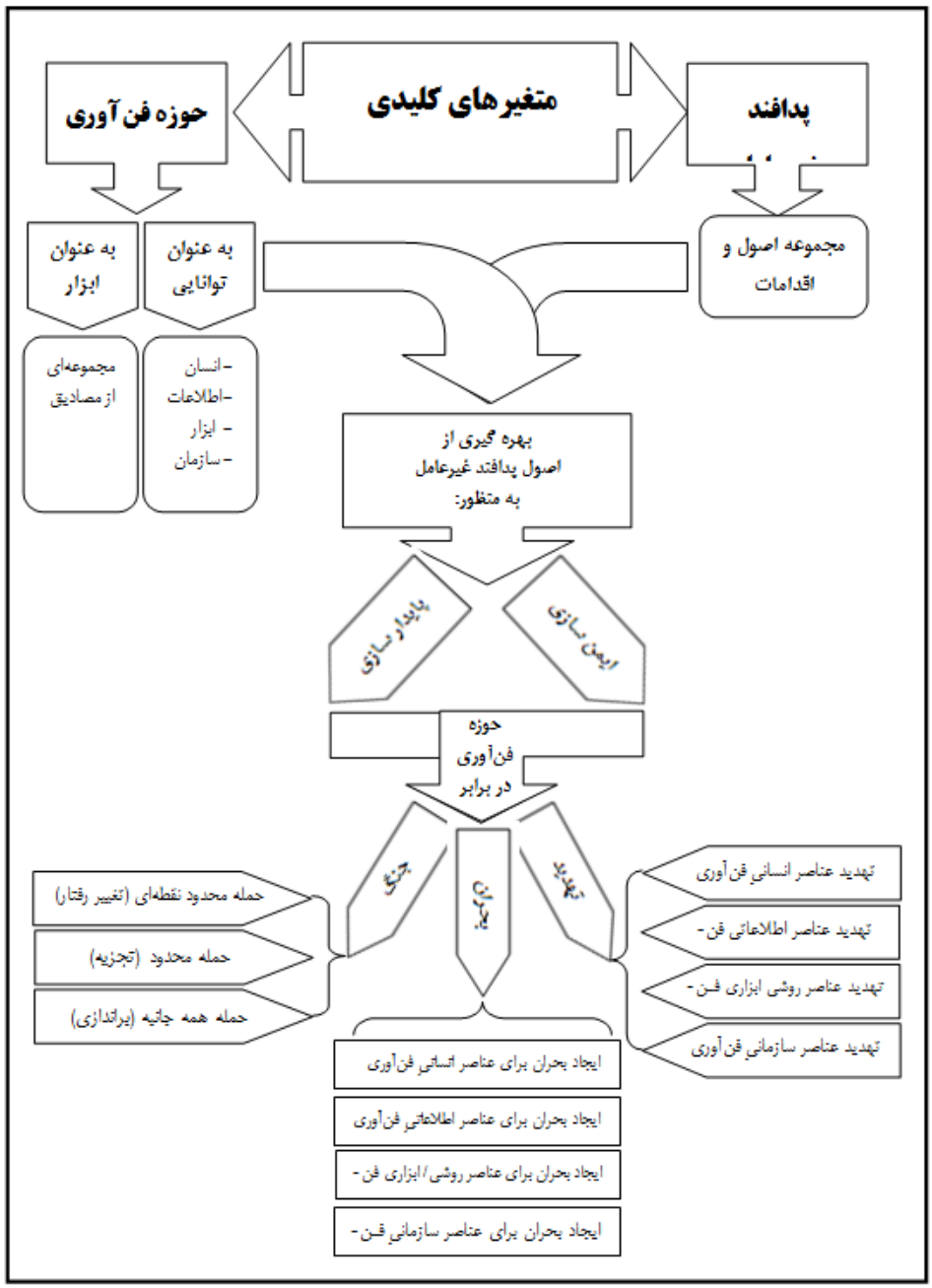
از آن‌جا که در شدیدترین حالتِ یک تهدید، یعنی وقوع جنگ، کلیه‌ی عناصر، بنیان‌ها و زیرساخت‌های فن‌آورانه‌ی یک کشور مورد تهاجم جدی قرار می‌گیرد، لذا در این تحقیق، حادترین وضعیت ممکن برای حوزه‌ی فن‌آوری یعنی وقوع جنگ خارجی، مدنظر قرار گرفته که با توجه به سناریوهای تهدید (perkovich, 2006: 19) و (Chossudovsky, 2012: 22)، چنین تهاجمی از سوی دشمن، حداقل به سه شکل مختلف می‌تواند جامه‌ی عمل بپوشد:

۱) حملات محدود و نقطه‌ای به اهدافی خاص در عرصه‌ی فن‌آوری، به منظور ایجاد تغییر رفتارِ در کشور هدف،

۲) حمله‌ی محدود؛ با هدف تجزیه‌ی بخش‌هایی از کشور،

۳) تهاجم همه جانبه با هدف براندازی کلیّت حاکمیت کشور.

مدل مفهومی پدافند غیرعامل در حوزه فن‌آوری



روش شناسی تحقیق

این تحقیق با توجه به ماهیت، ویژگی‌ها، اهداف و سؤالات مربوط به آن از نوع کاربردی - توسعه‌ای و روش تحقیق از نوع موردی و زمینه‌ای است. در این تحقیق، بیست نفر از کسانی که در هر دو حوزه‌ی پدافند غیرعامل و فن‌آوری صاحبنظر بوده‌اند به عنوان جامعه‌ی آماری در تعیین راهکارها و راهبردهای ایمن‌سازی و پایدارسازی عناصر چهارگانه‌ی فن‌آوری، همکاری داشته‌اند. روش نمونه‌گیری نیز تصادفی طبقه‌ای و جمع‌آوری اطلاعات به روش کتابخانه‌ای (بررسی اسناد و مدارک- آرشیو و کتاب) و نیز روش میدانی (مصاحبه و پرسشنامه) انجام شده است. تجزیه و تحلیل داده‌ها هم با استفاده از روش‌های آمار توصیفی و استنباطی و استفاده از روش‌های متداول در تدوین راهبرد انجام شده است.

همچنین روایی[1] پرسشنامه با طرح پرسش‌های صحیح و بدون ابهام (که جنبه‌ی مهمی از هدف تحقیق را تأمین نماید) و ارجاع مجدد پرسشنامه‌ها و مقایسه‌ی نتایج آن‌ها و از طریق اجرای روش ترستون[2]، تأمین شده است. بر پایه‌ی این روش، سؤالات پرسشنامه به وسیله‌ی ۵ نفر مورد بررسی قرار گرفت و پایائی مصاحبه به وسیله‌ی ایجاد روابط مطلوب با مصاحبه شونده و استوار نمودن مصاحبه بر مبنای یک ساختار، انجام شده است تا دستیابی به اطلاعات مهم را تضمین نماید و این کار با طراحی مجدد پرسشنامه‌ها به گونه‌ای دیگر، و در زمانی دیگر از طریق تکرار انجام مصاحبه توسط چند مصاحبه کننده تأمین گردید. با این روش، هماهنگی درونی آزمون تعیین شد و برای محاسبه‌ی قابلیت اعتماد (پایایی)[3]؛ سؤالات آزمون پس از مدتی به پرسش شوندگان داده شد و همبستگی بین پاسخ‌ها نیز مورد بررسی و تأئید قرار گرفت.

تجزیه و تحلیل محیط داخلی و خارجی در حوزه فناوری

بررسی عوامل داخلی

عوامل داخلی حوزه‌ی فن‌آوری، متغیرها و عواملی هستند که خود به دو دسته‌ی قوت‌ها و ضعف‌ها به شرح زیر تقسیم می‌شوند:

1 - Validity
2 Terston
3 - Reliability

بررسی نقاط قوت

نقاط قوت حوزه‌ی فن‌آوری به عوامل مؤثری اتلاق می‌شود که به‌طور رسمی و به عنوان مزیت و شایستگی‌های منحصر به فرد آن به‌شمار می‌آیند. به گونه‌ای که تقویت و توسعه‌ی این عوامل موجب ارتقاء سطح کیفیت، بهروری و امنیت عناصر فن‌آورانه می‌گردد. نقاط قوت حوزه‌ی فن‌آوری در چهار بعد به شرح زیر بیان شده است:

– **قوت‌های انسانی:** برخوردار از نیروهای انسانی فکری، علمی، مستعد، با انگیزه، مجرب و خودباور در کشور به‌عنوان واقعیت‌های جمعیتیِ قدرت‌ساز و قابلیت‌ساز در حوزه‌ی فن‌آوری.

– **قوت‌های اطلاعاتی:** در دستور کار قرار گرفتن فرهنگ‌سازی عمومی در خصوص تشریح ادبیات، اصول و مبانی پدافند غیرعامل در بخش‌های مختلف علمی، فنی و صنعتی و... . همچنین تلاش به‌منظور شناسایی نقاط قوت و ضعف فناوری دشمن، پیگیری مستمر رویکردها و روندهای فن‌آورانه‌ی دشمن. استفاده از طرح‌ها و تجربیات ارزشمند دوران مقدس.

– **قوت‌های ابزاری/ روشی:** ایده پردازی، طراحی و اجرای طرح‌های نوین در حوزه‌ی فن‌آوری مبتنی بر خلاقیت و روحیه‌ی خودجوشی و بومی. در دستور کار قرار گرفتن ایجاد زیرساخت‌های فنی لازم برای کاهش فاصله و «شکاف دیجیتالی» کشور با استانداردهای فنی تعریف شده‌ی جهانی. وجود گرایش و جذابیت ذاتی در موضوع و حوزه‌ی فن‌آوری به‌ویژه برای نیروهای جوان و دانشگاهی کشور.

– **قوت‌های سازمانی:** تدوین و تصویب سند چشم انداز بیست ساله‌ی کشور و توجه و تأکید بر جایگاه علمی و فنی جامعه‌ی ایرانی در افق آینده و برخوردار از دانش پیشرفته و توانا در تولید علم و فن‌آوری، متکی بر سهم برتر منابع انسانی و سرمایه های اجتماعی در تولید ملی– تدوین سند راهبردی ملی پدافند غیرعامل کشور– بهرمندی از اختیارات و حمایت‌های قانونی – توجه و اشارات روشن سیاست‌های امور فرهنگی، علمی و فناوریِ برنامه‌ی چهارم توسعه، نسبت به حوزه‌ی فناوری – تأکید و توجه به نقش دانش و علوم و فنون روز در اندیشهٔ حضرت امام خمینی(ره) – تدابیر مقام معظم رهبری پیرامون تحقیق و پژوهشِ علمی، دانش بومی، بهره‌گیری از ظرفیت‌ها و استعدادهای سرشار داخلی و منابع علمی و پژوهشیِ روزِ دنیا در راستای اهداف بلند اسلامی و انسانی. (امام خامنه‌ای، ۱۳۸۹/۸/۱۹– ۱۳۸۹/۲/۱۵– ۱۳۸۸/۸/۶– ۱۳۸۶/۷/۹ و ...) – تشکیل کمیته/سازمان دائمی پدافند غیرعامل کشور و پیگیری موضوعات مرتبط با طرح‌های پدافند

غیرعامل در حوزه‌های مختلف علمی، فنی و صنعتی- تصویب و تشکیل کمیته‌های پدافند غیرعامل در وزارتخانه‌ها و مؤسسات دولتی در خصوص پیگیری مباحث مرتبط با طرح‌های پدافند غیرعامل در عرصهٔ مطالعات فنی، تحقیق و توسعه- تصویب اصول پدافند غیرعامل مرتبط با حوزه‌های مختلف (از جمله فناوری) در سطح مدیریت کلان کشور (مجمع تشخیص مصلحت نظام) - تکمیل و اجرای نقشهٔ علمی کشور (سیاست‌های برنامه پنجم، ۱۳۸۷/۱۰/۲۱) به‌منظور ایجاد، تقویت وتوسعه‌ی زیرساخت‌های تحقیق و توسعه[1] کشور- بهره‌مندی از ساختار و آمادگی سازمانی نسبتاً مناسب و سامان یافته در دستگاه‌های اجرایی ذیربط.

بررسی نقاط ضعف

نقاط ضعف فن‌آوری کشور در چهار بعد فن‌آوری (یعنی ابعاد انسانی، اطلاعاتی، ابزاری و سازمانی)، به دست آمد که به دلیل رعایت مسائل حفاظت اطلاعات، علی‌رغم این‌که در تدوین راهبردها، منظور گردیده‌اند ولی از ذکر آن‌ها خودداری شده است.

بررسی عوامل خارجی

عوامل خارجی حوزه‌ی فن‌آوری، متغیرها و عواملی را شامل می‌شوند که خود به دو دستهٔ فرصت‌ها و تهدیدها به شرح زیر تقسیم می‌شوند:

بررسی فرصت‌ها

اهم فرصت‌ها در حوزه‌های چهارگانه‌ی فن‌آوری به شرح زیر می‌باشد:

- **فرصت‌های انسانی:** ایجاد جاذبه‌ها و زمینه‌های لازم در خصوص تحقق فرآیند مهاجرت معکوس (پذیرش مهاجرین نخبه‌ی خارجی) و استفاده از تجربیات و توانمندی‌های علمی و تحقیقاتی آن‌ها در داخل کشور- بهره برداری از توانمندی‌های نیروهای مازاد متخصص و محقق داخلی در خارج از کشور - برخوردار از نیروهای انسانی متخصص، کارآمد و «استعدادهای وافر و جوشان» (امام خامنه‌ای، ۱۳۸۴/۷/۲۱) به‌عنوان مزیت رقابتی ایران در تولید علم و صادرات نرم‌افزار[2].
- **فرصت‌های اطلاعاتی:** امکان نفوذ و رخنه در جامعه‌ی اطلاعات علمی، آموزشی، تحقیقاتی و فنی دشمن و نیز بهره‌برداری هدفمند از اطلاعات فنی آشکار آن‌ها - تحمیل آسیب پذیری‌ها و نقاط ضعف فناوری به دشمن به‌عنوان کشوری «فرو رفته در تکنولوژی»[3] - انتقال، انتشار و تکثیر و

1- R&D
2 - Software Exports
3- Over Reliance of Technology

صدور دانش فنی و بسته‌های اطلاعاتی هدفمند به مراکز و مخاطبان در اقصی نقاط جهان – تبادل اطلاعات و به هنگام سازی آخرین داده‌ها و اطلاعات علمی و تحقیقاتی از طریق تعامل و ارتباط با مراکز علمی، آموزشی، تحقیقاتی سایر کشورها.

– **فرصت‌های ابزاری:** وابستگی شدید نظام جامع اطلاعاتی (اطلاع گیری و اطلاع رسانی) دشمن به سیستم‌ها، سخت‌افزارها و ابزارهای فناورانه.(Sechrist, 2012: 15) – اختلال‌پذیر بودن زیرساخت‌های شبکه‌ای و نظام سیستماتیک دشمن(McGuinn, 2004: 6) .

– **فرصت‌های سازمانی:** عزم دولت (منبعث از سند چشم انداز) برای مشارکت فعال در طراحی و اجرای پروژه‌های پدافند غیرعامل با رویکرد فناورانه در موضوعاتی که بیش از همه به طور مستقیم با امنیت ملی (حال و آینده) کشور ارتباط دارد – آمادگی بخش دولتی در سرمایه‌گذاری در آن دسته از پروژه های پدافند غیرعاملی که نیازمند ضریب بالایی از خطر و ریسک پذیری در حوزه‌ی فن‌آوری می‌باشد – وجود روحیه‌ی تحرک (امام خامنه‌ای، ۱۳۶۸/۳/۱۷)، خودجوشی (امام خامنه‌ای، ۱۳۷۸/۵/۸) و خودایستایی در حوزه‌های مختلف علمی، فنی، تحقیقاتی و... ناشی از تحریم کشور توسط سایر کشورها و نهادهای بین‌المللی.

بررسی تهدیدها

تهدیدهای حوزه‌ی فن‌آوری در ابعاد انسانی، اطلاعاتی، ابزاری و سازمانی عبارت است از:

– **تهدیدهای انسانی:** توان دشمن در استفاده از ابزارهای فناورانه‌ی عملیات روانی(امام خامنه‌ای، ۱۳۸۷/۳/۱۴)، (Reimer, 2007: 26) و تلاش برای ایجاد تزلزل در ارزش‌ها، اندیشه‌ها و نگرش‌های محققان و متخصصان کشور و نیز تلاش به‌منظور «فرار مغزها» (امام خامنه‌ای، ۱۳۸۳/۹/۲۶) و قطع نمودن پیوند منفعتی بین دولت – ملت و نیروهای متخصص به عنوان «ثروت ملیِ انسانی» (امام خامنه‌ای، ۱۳۸۱/۷/۳) و پیوند دادن آن‌ها با منافع و هویت‌های فراملی، همچنین تلاش وی در ملیت زدایی[1]، سرزمین زدایی[2]، یا مکان زدایی[3]، قشر نخبه و تحصیل‌کردهٔ کشور و «ربودن مغزها» (امام خامنه‌ای، ۱۳۷۰/۱۱/۳۰) یا ایجاد میل و رغبت در آن‌ها به‌منظور خروج از کشور از طریق، تبلیغ، ترویج و تلقین یکسری «عوامل کِششی» و جاذبه‌های علمی، تحقیقاتی مانند:

– امکانات علمی، آموزشی، تخصصی، تحقیقاتی و توسعه‌ای بیشتر در خارج از کشور،

1 - Denationalization
2 - Detritorization
3 - Delocalization

- احساس آرامش، ترقی، توسعه و ثبات در امور تحصیلی، اجتماعی و شخصی،
- فرصت‌های شغلی، کاری و امکانات رفاهی و تفریحی بیشتر،
- تسهیلات روادید و اقامت،
- امکان مشارکت در امور تحصیلی، تحقیقی، تخصصی و مدیریتی،
- امکان تحرک شغلی بیشتر و بهتر،
- احساس منزلت اجتماعی بیشتر و پذیرفته شدن در جامعه،
- سنخیت و تناسب بیشتر شغل و تحصیل با یکدیگر،

- محدود و محصور نمودن نیروهای فنی، متخصص و فکور کشور از طریق اعمال یکسری محدودیت‌ها یا ممنوعیت‌های منطقه‌ای یا جهانی (مثل تهدید، ترور، تحریم، ممنوع الخروج نمودن و...) و از بین بردن فرصت‌های علمی و تحقیقاتی جهانی از آن‌ها و استفاده از ابزارها، نهادها و سازمان‌های بین‌المللی به‌منظور تحت فشار قرار دادن فعالیت آن‌ها.(Cordesman, 2013: 3)

- **تهدیدهای اطلاعاتی:** تلاش و توان دشمن در «مفهوم سازی»[1] و ایجاد جنگ روانی[2] علیه فعالیت‌های علمی، تحقیقاتی، صنعتی کشور و معادل‌سازی فناوری‌های پیشرفتهٔ ایران با عناوینی همچون فناوری‌های تروریستی(Cordesman, 2006: 31)، تسلیحات کشتار جمعی[3] (Salsbilit, 2013: 3صنایع تهدید کنندهٔ محیط زیست، اقدامات ضد حقوق بشر، فناوری‌های تهدیدکنندهٔ صلح و امنیت همسایگان، منطقه، جهان و ... (Sherrill, 2012: 31). - توان دشمن در توسعهٔ طرح‌ها و ایده‌های تحقیقاتی تخیلی، نوآورانه و اغلب با ضریب ریسک بسیار بالا و با تاثیرات فناورانه‌ی زیاد و تلاش برای تبیین و تحقق آن از امکان‌پذیری فنی تا توسعهٔ سیستم‌های نمونه. - توان و تلاش دشمن (به‌عنوان یکی از پتانسیل‌های عظیم ژئوپلیتیک قدرت و فن‌آوری در جهان) به‌منظور کانالیزه و «انحصار فن‌آوی» (امام خامنه‌ای، ۱۳۸۲/۱۱/۲۱) در جهان از طریق مجاری، مجامع و مؤسسات بین‌المللی. - توان و تلاش دشمن در تغییر، تحریف، سیاه نمایی، کم ارزش یا بد جلوه دادن و منحرف نمودن ذوق و ذائقه‌های علمی، آموزشی، تربیتی و تحقیقاتی نخبگان و صاحبنظران بومی کشور و ترغیب و تشویق آن‌ها در گرایش به سمت اندیشه‌ها و ارزش‌های غربی از طریق انتشار حجم بالایی از اطلاعات آلوده از کانال خبرگزاری‌ها، شبکه‌های ماهواره‌ای و سایر رسانه‌های

1- Conceptualization
2- Psychological Warfare
3- WMD: Weapons of Mass Destruction

اطلاعـــاتی و ارتباطـــاتی جهـــانی. (امـــام خامنـــه‌ای، ۱۳۷۳/۴/۲۹ – ۱۳۷۰/۱۰/۲۵– ۱۳۹۰/۶/۱۷– ۱۳۹۰/۶/۲ –۱۳۸۷/۶/۳۰)

– **تهدیدهای ابزاری:** توان دشمن در کاهش زمان تحقیق و توسعه و تبدیل «فناوری بـه سیسـتم و محصول» در حداقل زمان ممکن. – استفاده از شبکه‌های اطلاعاتی و ارتباطی جهان گستر (همچون اینترنت) به‌عنوان ابزاری برای تأمین اهداف سیاست خارجی آمریکا در ورای مرزهـای جغرافیـایی بر اساس چشم انداز استراتژی امنیت ملی آمریکـا بـرای قـرن ۲۱.(Solomon, 2000: 40) – تـوان دشمن در بهره برداری از سیستم‌های پاسخگوی واکنش سریع (آنی)[1] به کمک حسگرهای پیشرفته و پردازشگرهای اطلاعاتی فوق سریع و برتری اطلاعاتی[2] در بسیاری از عرصه‌های زمینی، دریـایی، هوایی، فضایی و سایبری. (perry, 2004: 7) – توجه، تمرکز و تأکید دشمن بر «علم و فناوری» بـه جای «تحقیق و توسعه» و تأکید ویژه بـر اصـل «دسـتیابی» در طـرح‌هـا و پـروژه هـای تحقیقـاتی. (Blanpied, 2008: 30).

– **تهدیدهای سازمانی:** توان و تسلط دشمن بر برخی موسسات مطرح بین المللی (همچون ISI[3] ، ISO[4] و...) در راستای نظارت و کنترل (جاسوسی) بر منابع علمی، فنی، صنعتی، تحقیقاتی کشورها (از جمله ایران) و پیگیری روند رشد و جهت گیری آن‌ها. – توان دشمن در پـیش‌بینـی، پیگیـری، تقویت و توسعه‌ی فرصت‌های نوین و سرمایه گذاری‌های علمی و تحقیقـاتی(NSF, 2014: 13)، و تفکرات اثرپایه[5] و دستیابی به آخرین اکتشافات و نـوآوری‌هـای علمـی و فنـی در راسـتای ایجـاد تغییرات ذهنیتی و نگرشی، به‌منظور مرتفع‌سازی نیازهای ملی و تأمین تقاضـاهای پنهـان کشـور در بخش فناوری طی دهه‌های آینده.– توان و تلاش هدفمند اندیشگاه‌ها[6] و مراکز تحقیق و توسـعه‌ی[7] دشمن به‌منظور شناسایی و افزایش شکاف منفعتی بین دولت و ملت و نیز بین بـازیگران دولتـی و غیردولتی کشور و تحلیل و تضعیف مؤلفه‌های مختلف مفاهیمی همچون قدرت ملی، منـافع ملـی، اهداف ملی، امنیت ملی، دفاع ملـی و ... در کلیـه‌ی حـوزه‌هـا از جملـه حـوزه‌ی علـم و فنـاوری.

1 - Rapid Response System
2- Information Superiority
3 - Information Sciences Institute
4 - International Organization for Standardization
5 - Effects – Based Thinking
6 - Think Tanks
7 - Research and Development Centers

(Green, 2009: 5) و (Crane, 2008: 67-105) – توان اثرگذاری بر نهادهای بین‌المللی و اعمال برخی تحریم‌ها از سوی دشمن و ممانعت از دسترسی ایران به برخی از ظرفیت‌های علمی و فنی لازم در حوزه‌ی فناوری. (PASIA: 2012: 9).

پس از بررسی و احصاء عوامل محیط داخلی (قوت‌ها و ضعف‌ها) و نیز عوامل محیط خارجی (فرصت‌ها و تهدیدها)، چهار «ماتریس ارزیابی محیطی» (دو ماتریس برای ارزیابی عوامل محیط داخلی و دو ماتریس نیز برای ارزیابی عوامل محیط خارجی) به صورت جداگانه تهیه و از بیست نفر از صاحب‌نظران حوزه‌ی فناوری و پدافند غیرعامل خواسته شد تا نظرات خود را در خصوص هر یک از موارد خواسته شده در جدول، بر اساس ضریب از ۱ تا ۱۰ برای ستون «میزان اهمیت» و «میزان بهره‌گیری»، ارائه نمایند. بر این اساس مجموعا ۴۰ جدول به دست آمد.

منظور از «میزان اهمیت» در هر یک از جداول؛ میزان تأثیری است که هر عامل در تدوین راهبرد پدافند غیرعامل در حوزه‌ی فناوری دارا می‌باشد. این میزان تأثیر از عدد ۱ تا ۱۰ متغیر بوده و ضریب ۱ برای عواملی که کمترین تأثیر (مثبت یا منفی) و عدد ۱۰ برای عواملی که بیشترین تاثیر (مثبت و منفی) را در تدوین استراتژی دارا می‌باشند، منظور شده است.

همچنین منظور از «میزان بهره‌گیری» در هر یک از جداول؛ میزان توانایی کشور در بهره‌برداری از قوت‌ها و فرصت‌ها و نیز میزان توانایی پاسخگویی و مقابله با ضعف‌ها و تهدیدها می‌باشد. میزان بهره‌گیری نیز از عدد ۱ تا ۱۰ متغیر بوده و عدد انتخابی توسط پرسشگران بیانگر میزان اثربخشی استراتژی‌های «حال و آینده» در کشور نسبت به عامل مزبور می‌باشد.

مجموع نتایج به دست آمده، ابتدا در ۴۰ جدول گردآوری و سپس در چهار جدول با عنوان قوت-ها، ضعف‌ها، فرصت‌ها و تهدیدها تنظیم گردید و در ادامه، «میانگینِ» سه ستون از جدول مذکور، یعنی ستون‌های: «میزان اهمیت»، «میزان بهره‌گیری برای وضع موجود» و «میزان بهره‌گیری برای وضع مطلوب» محاسبه و نتایج حاصله در چهار جدول دیگر (بر اساس همان الگو) منظور شد و در ادامه، دو ستونِ «جمع موزون برای وضعیت جاری و مطلوب»، از طریق ضرب مقادیر ستونِ «میزان اهمیت» در مقادیر ستونِ «میزان بهره‌گیری» و درج آن در ستون «جمع موزون»، انجام شد. که بر این اساس چهار جدول دیگر (برای قوت‌ها، ضعف‌ها، تهدیدها و فرصت‌ها) به دست آمد.

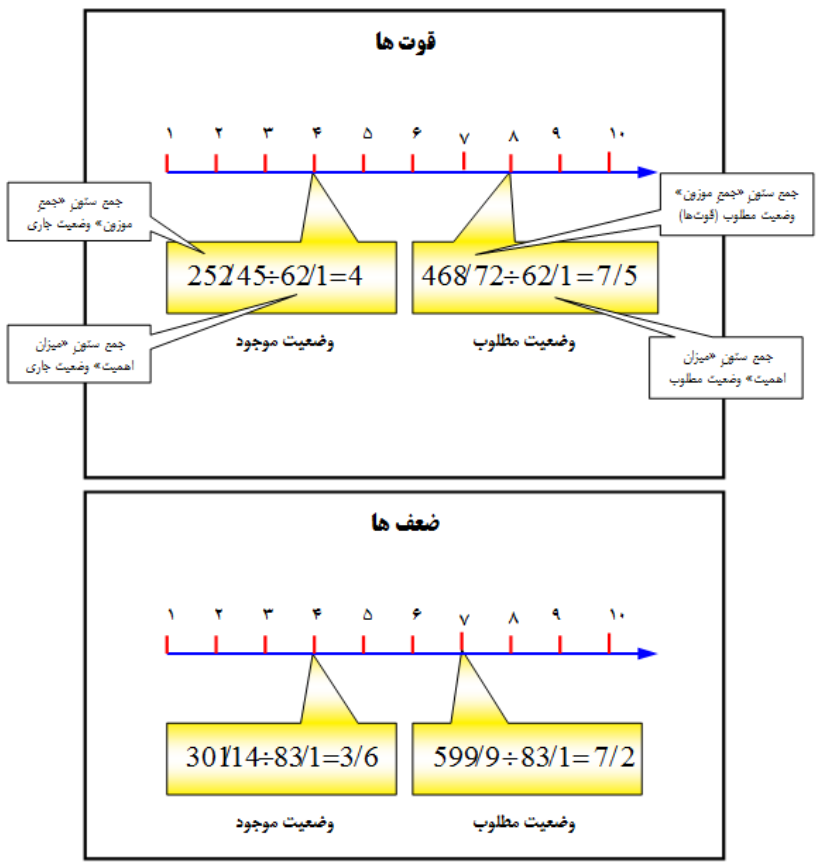
سپس بر اساس جدول شماره ۱، مستخرجه از عملکرد و نتایج فوق، چهار نمودار (نمودارهای ۴-۱) با عنوان «نمودار میزان بهره برداری از قوت‌ها، ضعف‌ها، تهدیدها و فرصت‌ها در وضعیت

موجود و مطلوب» ترسیم شد. برای این کار جمعِ ستون «جمعِ موزونِ وضعیت جاری» و نیز جمع ستونِ ««جمعِ موزونِ وضعیت مطلوب» را تقسیم بر جمع ستون «میزان اهمیت» نمـوده و آن را در محور مختصات مربوط به قوت‌ها، ضعف‌ها، تهدیدها و فرصت‌ها، نمایش داده شده است:

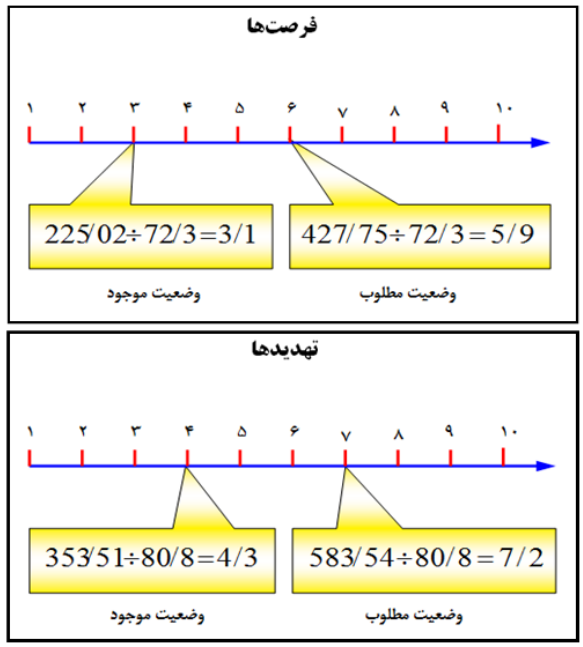
جدول شماره (۱)

	وضع موجود	وضع مطلوب
قوت‌ها	۴	۷/۵
ضعف‌ها	۳/۶	۷/۲
فرصت‌ها	۳/۱	۵/۹
تهدیدها	۷/۲	۴/۳

نمودارهای شماره (۱ و ۲): میزان بهره برداری از قوت‌ها و ضعف‌ها در وضعیت موجود و مطلوب



نمودارهای شماره (۳ و ۴): میزان توان بهره‌برداری از فرصت‌ها در وضعیت موجود و مطلوب



«ماتریس ارزیابی اقدام و موقعیت استراتژیک» (یا به اصطلاح ماتریس SPACE)، که به منظور تعیین استراتژی‌های مختلف برای موقعیت‌های متفاوت فراهم شده، در این مقاله بر اساس چهار بُعد «قوت‌ها– ضعف‌ها– تهدیدها و فرصت‌های فناوری» تنظیم شده است. استراتژی‌های بدست آمده در این ابعاد نیز که عبارتند از: استراتژی تهاجمی[۱]، استراتژی تدافعی[۲]، استراتژی رقابتی[۳] و استراتژی محافظه کارانه[۴]، در نمودار (۵) آمده است.

در این تحقیق، چهار پرسشنامه (پیرامون قوت‌ها، ضعف‌ها، تهدیدها و فرصت‌ها) به صاحبنظرانی در «حوزه‌ی فناوری و پدافند غیرعامل» داده شد که به آن‌ها پاسخ داده‌اند. سپس با استفاده از ماتریس ارزیابی اقدام و موقعیت استراتژیک، موضع و موقعیت حوزه‌ی فناوری مشخص شده است. بر این اساس با توجه به این نکته که حوزه‌ی فناوری، در کدامیک از موقعیت‌های تعیین شده در ماتریس، قرار بگیرد، استراتژی متناسب با آن موقعیت، ارائه شده است.

1- Aggressive Strategy
2- Defense Strategy
3- Competitive Strategy
4- Conservative Strategy

در این تحقیق برای استفاده از روش تحقیق مناسب، از روش آماری میانگین موزون استفاده شده است.

با توجه به جداول به‌دست آمده از ماتریسِ ارزیابی اقدام و موقعیت استراتژیک، (وضعیت موجودِ) حوزه‌ی فناوری در ماتریس SPACE در موقعیت «استراتژی تدافعی» قرار گرفت و این به معنای بدترین، دشوارترین و مخاطره آمیزترین شرایط برای حوزه‌ی فناوری است. زیرا، علی‌رغم آن که این حوزه با ضعف‌ها و ناتوانی‌های متعدد و قابل توجهی مواجه است، در محیط‌های تعاملی یا زمینه‌ای خود نیز با فشارها، چالش‌ها و تهدیدهای گوناگونی باید مقابله نماید. از این رو، باید با استفاده از راهبردهای (WT)، نقاط ضعف حوزه‌ی فناوری، پوشش داده شود یا آسیب‌پذیری‌های آن از ناحیه‌ی تهدیدهای محیطی، کمینه و به حداقل ممکن رسانده شود.

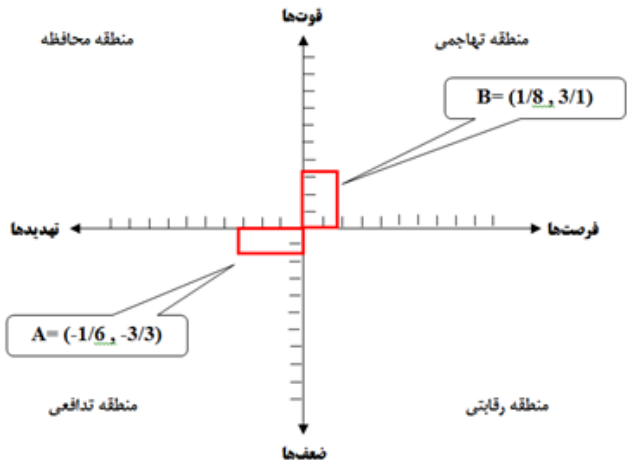
استراتژی مناسب (مطلوب) برای آینده‌ی حوزه‌ی فناوری، استراتژی تهاجمی (SO) است که مطلوب‌ترین حالت ممکن می‌باشد و بدین معنی است که حوزه‌ی فناوری کشور ضمن آن‌که باید از توانایی‌ها و نقاط قوتِ درخور و قابل اتکایی برخوردار باشد، در محیط تعاملی و زمینه‌ای خود نیز با فرصت‌های مناسب و گرانبهایی مواجه است که باید بتواند از آن‌ها حداکثر استفاده را به عمل آورد. این دسته از راهبردها چگونگی به کارگیری توان موجود در حوزه‌ی فناوری را جهت بهره برداریِ حداکثری از فرصت‌های مغتنم محیطی بیان می‌دارند.

موقعیت حوزه‌ی فن‌آوری در وضعیت موجود و مطلوب، با توجه به داده‌های به‌دست آمده در جدول شماره ۲، در نمودار ۵، ترسیم شده است.

جدول شماره (۲): تعیین موقعیت در وضعیت موجود و مطلوب

وضعیت موجود	قوت + (تهدید -۱۰) = ٤ + (۷/۲ – ۱۰) = -۱/۶ فرصت + (ضعف -۱۰) = ۳/۱ + (۳/٦ – ۱۰) = -۳/۳	A = (-۱/6 و -۳/3)
وضعیت مطلوب	قوت + (تهدید -۱۰) = ۷/۵ + (٤/۳ – ۱۰) = -۱/۸ فرصت + (ضعف -۱۰) = ۵/۹ + (۷/۲ – ۱۰) = -۳/۱	B = (۱/۸ و ۳/۱)

نمودار (۵): نمودار ارزیابی موقعیت و اقدام استراتژیک (SPACE)[1]



نتیجه گیری و پیشنهادات

الف– نتیجه‌گیری

راهبردهای حوزه‌ی فناوری که بالاترین امتیازات را در نظرسنجی کسب نموده‌اند به ترتیب اولویت عبارتند از:

۱- ایجاد و ارتقاء ایده‌ها و جلوه‌های نوین پدافندی در حوزه‌ی فن‌آوری به‌منظور کاهش زمان «تحقیق و توسعه» و تسریع در تولید «علم و فن‌آوری» و دستیابی به «محصول و سیستم».

۲- شکوفاسازیِ نوآوری‌های فن‌آورانه از طریق ایجاد و پرورش حس تعلق، تعهد و منزلت اجتماعی در نیروهای نخبه به‌منظور ایجاد بازدارندگی و ممانعت از فرار مغزها.

۳- مقابله‌ی منسجم و مستمر با تهدیدات فناورپایه‌ی دشمن از طریق تولید، توسعه و تکمیل ابزار، فنون، مهارت‌ها و زیرساخت‌های امن، استاندارد و جایگزین پذیر در حوزه‌ی فن‌آوری.

۴- رفع موانع ساختاری و مدیریتی در زمینه‌ی شناسایی، ارزش گذاری، امکان سنجی و اولویت‌بندی اقدامات و الزامات حوزه‌ی فن‌آوری از منظر تهدیدشناسی.

۵- تقویت و توسعه‌ی کارآفرینی فنی و استمرار و استحکام فرآیند تولید علم و فن‌آوری در اندیشگاه‌ها و پژوهشگاه‌ها و دانشگاه‌های تخصصی از طریق شناسایی، جذب و بکارگیری منابع سرمایه‌ای (انسانی، اعتباری، فیزیکی) ملی و فراملی.

1 - *Strategic Position* Action and Evaluation Matrix

۶- بهره‌گیری از روش‌ها، ابزارها و زیرساخت‌های فن‌آورانه‌ی بومی، بدیع و به لحظه، به‌منظور ایجاد تعامل، تمرکز و تحکیم روابط با مخاطبین در اقصی نقاط جهان.

۷- تمرکز بر توانمندی‌ها، تفکرات و اطلاعات اثرپایه‌ی پدافندیِ به‌منظور تحمیل اراده و آسیب‌پذیری‌های فن‌آوری به دشمن.

۸- تقویت، توسعه، تداوم و بهره برداری از چرخه و نظام اطلاع رسانی و فرهنگ‌سازی ملی در زمینه‌ی سازگارسازی و مقاوم‌سازی عناصر فناورانه در برابر عوامل و فرآیندهای تهدیدساز.

۹- همگام و همگرا نمودن بخش‌های فن‌آورانه‌ی «علمی، اجرایی»، «دولتی، خصوصی» در مقیاس ملی، به‌منظور هم افزا نمودن نتایج راهبردها و بهره‌برداری از فرصت‌ها.

۱۰- هدایت و مدیریت منابع فن‌آوری۱ ملی با رویکرد آینده نگرانه.

۱۱- ایجاد و بهره‌برداری از بازدارندگی فناورانه، از طریق بهینه، روزآمد و نهادینه‌سازی اصول، ارزش‌ها، اهداف و اشراف اطلاعاتی و فنی.

۱۲- بهره‌گیری از قوانین، فرامین، تدابیر و سیاست‌های حمایتی و مدیریتی مصوب به‌منظور صدور دانش فنی، همسو با اهداف و منافع ملی.

۱۳- استفاده از ظرفیتِ‌های توسعه یافته در حوزه‌ی فناوری‌های نوظهور به‌منظور مقابله با مراکز و سیستم‌های پشتیبانی کننده‌ی تصمیم‌گیر و تهدیدساز دشمن.

۱۴- بهره‌برداری از تحقیقات، تجربیات و تعاملات متقابل با جامعه‌ی اطلاعات جهانی به‌منظور رفع خلاءهای علمی و دستیابی به الگوها و آموزه‌های نوین در حوزه‌ی فن‌آوری.

۱۵- عمق‌بخشی خارجی در حوزه‌ی فن‌آوری‌های نوظهور کاهش و رفع ضعف‌های حوزه‌ی فن‌آوری از حیث ابزارشناسی، روش شناسی و مهارت‌ورزی

ب- پیشنهادها

اجرایی و عملیاتی نمودن راهبردهای فوق الاشاره، خود نیازمند الزاماتی به شرح زیر می‌باشد:

۱- تقویت عزم، اراده، خودباوری و انگیزه‌های ملی در مراکز علمی و فنی.

۲- اجرا، اصلاح یا وضع قوانین جدید؛

۳- پژوهش محور نمودن مراکز علمی؛

۴- سیاستگذاری و اولویت‌بندی ضرورت‌های علمی - فنی؛

1 - TRM: *Technology Resource Management*

۵- ارتباط مستمر با مراکز علمی و فنی؛
۶- تأمین و تقویت مالی طرح‌های تفکرپایه؛
۷- اجرای نظام جامع علمی کشور؛
۸- حمایت از محصولات و نوآوری‌های علمی- فنی؛
۹- آزمون میزان اثرگذاری و صحت عملکرد عناصر حوزه‌ی فناوری؛
۱۰- تسهیل فرآیندها، راهکارها و ساز و کارهای اجرایی و هدفمند برای سازمان‌های دانش بنیان؛

فهرست منابع

الف– منابع فارسی

- خلیل، طارق (۱۳۸۳)، مدیریت تکنولوژی، رمز موفقیت در رقابت و خلق ثروت، ترجمه: اعرابی، سید محمد و ایزدی، داود، تهران، دفتر پژوهش‌های فرهنگی.
- سیاست‌های کلی علم و فناوری، ابلاغی از سوی مقام معظم رهبری، مورخه ۱۳۹۳/۶/۲۹.
- سیاست‌های کلی برنامه پنجم توسعه، ابلاغی از سوی مقام معظم رهبری، مورخه ۱۳۸۷/۱۰/۲۱.
- سیاست‌های کلی نظام در خصوص پدافندغیرعامل، سایت مقام معظم رهبری؛ ۱۳۸۹/۱۱/۲۹:
- http://farsi.khamenei.ir/
- مجموعه مقالات دومین همایش علم و فناوری (۱۳۸۲)، مرکز تحقیقات استراتژیک، معاونت علوم و تکنولوژی.
- نرم افزار حدیث ولایت (مجموعه بیانات رهبر معظم انقلاب حضرت آیت الله امام خامنه‌ای).

ب– منابع انگلیسی

- Chossudovsky, Michel (2012) Towards a World War III Scenario? The Role of Israel in Triggering an Attack on Iran**,** [online] https://store.globalresearch.ca/store/towards-a-world-nuclear-war/
- Cordesman, Anthony (2006) Iranian Nuclear Weapons? The Threat from Iran's WMD and Missile Programs, available at:
  - http://csis.org/files/media/csis/pubs/060221_iran_wmd.pdf
- Cordesman, Anthony (2013) U.S. and Iranian Strategic Competition; Sanctions, Energy, Arms Control, and Regime Change, Center for Strategic and international Studies: http://csis.org/files/publication/120124_Iran_Sanctions.pdf
- Cornish, Paul (2010) On Cyber Warfare, available at:
  - https://www.chathamhouse.org/sites/files/1110_cyberwarfare.pdf
- Crane, Keith (2008) Iran's Political, Demographic, and Economic Vulnerabilities, available at: http://www.rand.org/MG693.pdf
- Gancia, Gino (2008) Technological Change and the Wealth of Nations, available at: http://www.crei.cat/people/GZannrev.pdf
- Govindaraju, Rajesri (2010) Analysis of the Influence of Technology on the Business, available at: http://apiems.net/archive/apiems2010/pdf/SE/128.pdf
- Green, Jerrold (2009) Understanding Iran, available at: http://www.rand.org/content/dam/rand/pubs/RAND_MG771.pdf
- Haeni, Reto E. (1997) Information Warfare an introduction, The George Washington University, available at: http://www.trinity.edu/rjensen/infowar.pdf
- McGuinn, Martin G. (2004) Prioritizing Cyber Vulnerabilities, available at: http://www.dhs.gov/ NIAC_CyberVulnerabilities.pdf
- Molander, Roger C. (1996) Strategic Information Warfare: a new face of war, National Defense Research Institute, available at: http://www.rand.org/content/rand_reports/2005/MR661.pdf
- Perkovich, George (2006) Five Scenarios for the Iranian Crisis, Security Studies Department, available at*:* www.ifri.org/

- Perry, Walter (2004) Exploring Information Superiority, A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness, National Defense Research Institute, available at: http://www.rand.org/content/2005/MR1467.pdf
- Raushenbakh, Boris V. (2010) Computer War, available at: http://www-ee.stanford.edu/Breakthrough/book/pdfs/raushenbakh.pdf
- Reimer, Dennis (2007) Psychological Operations Process: Tactics, Techniques, and Procedures, FM 3-05.301, available at**:** http://info.publicintelligence.net/USArmy-PsyOpsTactics.pdf
- Rosenau, William (2006) Waging the ‘‘War of Ideas’’, Georgetown University available at: ttp://www.rand.org/pubs/ RP1218.pdf
- , Dr.K (2014) Cyber War, Methods and Practice, University OSNABRUCk, available at: http://www.dirk-koentopp.com/methods-and-practice.pdf
- Salsabili, Mansour (2013) Iran and Weapons of Mass Destruction, the Military Dynamics of Nonproliferation, Harvard Kennedy School, available at: http://belfercenter.ksg.harvard.edu/files/salsabili-dp-march-2013.pdf
- Sechrist, Michael (2012) New threats, old technology Vulnerabilities in Undersea Communications Cable Network Management Systems, [online] http://ecir.mit.edu/images/stories/sechrist-dp-2012-03-march-5-2012-final.pdf
- Shaihebrew,Nachman (2013) Media War Reaching for Hearts and Minds, Publisher; yediot, available at: http://www.amazon.com/
- Shaw, John (2011) ‘Satellite Wars in the Middle East: A Battle for Hearts and Minds’ Durham University: https://www.dur.ac.uk/resources/MediaPoster22.pdf
- Sherrill, Clifton (2012) Why Iran Wants the Bomb and What IT Means for US Policy, available at: http://cns.miis.edu/iran_bomb.pdf
- Solomon, Richard H. (2000) U.S. Foreign Policy Agenda: The Internet and the Diffusion of Diplomacy, available at: http://guangzhou.usembassy-china.org.cn/uploads/images.pdf
- Streenhuis, Harm-Jan (2006) High Technology Revisited: Definition and Position, Eastern Washington University, [online] http://doc.utwente.nl/high_technology.pdf
- Work, Robert (2014) Preparing for War in the Robotic Age, Center for a New American Security, Available at: http://www.cnas.org/publications-pdf/WorkBrimley.pdf