مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی

محمدرضا مرادی[۱]، محمدرضا ولوی[۲]، متین مرادی[۳]

[۱] دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران
mr.moradi@sndu.ac.ir
[۲] دانشیار دانشگاه صنعتی مالک اشتر، تهران
valavi@mut.ac.ir
[۳] دانشجوی مهندسی نرم‌افزار کامپیوتر، دانشگاه شاهد ، تهران
matinmoradi1401@gmail.com

چکیده

دکترین در حقیقت، فلسفه را که اغلب ابهام‌آلود و نظری است، می‌گیرد و آن را عملیاتی می‌کند تا از دل آن، سیاست‌هایی خاص بیرون بیاید. در خصوص مفهوم دکترین در دنیا، تفاوت دیدگاه وجود دارد. رویکرد ج.ا.ا. به دکترین نیز، با دو رویکرد غالب شرقی و غربی تا حدودی متفاوت است. دکترین عمدتاً در امور دفاعی-امنیتی به‌کار می‌رود. کشورهای دنیا، برای تدوین دکترین از مدل‌های مشخصی بهره می‌برند که عموماً نیز این مدل‌ها به‌صورت واضح تشریح نمی‌گردند. فضای سایبر، پدیده نوظهوری است که دارای ویژگی‌های خاص خود می‌باشد. این فضا چند سالی است که رسماً به‌عنوان یکی از عرصه‌های جنگ تعریف گردیده است. بنابراین چنانچه در نظر داشته باشیم برای این فضا در حوزه دفاعی-امنیتی دکترین تدوین نماییم، نیازمند یک مدل خاص‌منظوره می‌باشیم. مدل فرآیندی معرفی شده، مختص فضای سایبر جمهوری اسلامی ایران است و برگرفته از یک کارپژوهشی گسترده (با بهره‌گیری از نظر خبرگان و تعیین اعتبارسنجی آن) است که نتیجه آن ارائه شده است. هدف این پژوهش که برگرفته از یک رساله دکتری می‌باشد آن است که مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی-امنیتی احصا شود.

کلمات کلیدی: دکترین، فضای سایبر، دفاعی امنیتی، تدوین مدل.

۱ مقدمه

در اداره امور یک کشور مهم‌ترین مسأله، حاکمیت است و حاکمیت نیازمند یکپارچگی است. پس از تدابیر منسجم متولیان حکومتی، سایرین در هر سازمان و دستگاهی می‌توانند به‌صورت هماهنگ و هم‌افزا اقدام نمایند. دکترین گفتمان مشترک ایجاد می‌نماید و این گفتمان مشترک می‌تواند به اقدامات هم‌سویی منجر شود

که ثمرات آن در اثر هم‌افزایی به‌صورت تصاعدی افزایش می‌یابد. سازمان‌های دفاعی-امنیتی در جمهوری اسلامی ایران پس از ورود عرصه سایبری به حوزه دفاع و امنیت، تلاش‌های فروانی در راستای مدیریت راهبردی این فضا به انجام رساندند. لیکن نقصان‌ها و چالش‌هایی در مدیریت کلان این فضا مشاهده می‌شود. تدوین دکترین در این حوزه امکان ایجاد وحدت رویه را فراهم می‌نماید؛ از آن جایی که تدوین دکترین، نیازمند یک الگو می باشد در این مقاله سعی داریم الگوی فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران را در حوزه دفاعی امنیتی ارائه نماییم. بدین منظور ابتدا به تبیین مفهوم دکترین می‌پردازیم سپس نگاهی گذرا به برخی مدل های تدوین دکترین سایبری در داخل و خارج از کشور می اندازیم در ادامه دکترین سایبری دفاعی امنیتی را تشریح می نماییم و در انتها به معرفی مدل می پردازیم. این مقاله بر اساس تعاریف مفاهیم زیر[۱] به‌وسیله محققین بنا شده است.

۲ دکترین

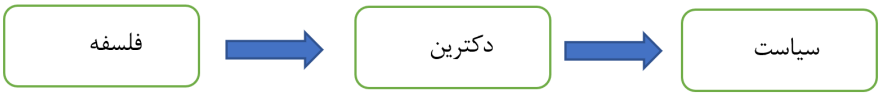
۱.۲ مفهوم دکترین

دکترین در معنای عام به معنای اعتقادات یا اندیشه‌هایی است که در یک مکتب فکری جایگاه برجسته‌ای دارد (دکترین مهدویت در شیعه). معنای خاص آن به معنای اصول و قواعدی است که در یک علم خاص همچون سیاست و اقتصاد جنبه کاربردی داشته باشد و باید در مقام عمل به‌کار بسته شود (دکترین چماق و هویج در سیاست [۲]). از میان معانی یادشده آنچه مدنظر محققان به‌عنوان تعریف عملیاتی است معنای دوّم دکترین است.

شناخت دکترین، از آنجایی شروع می‌شود که هر فلسفه و نظام شناختی، الزاماً برای پیاده شدن در متن اجتماع و بیان چگونگی حیات انسانی، نیاز به‌واسطه‌ای دارد. بر این اساس، دکترین موضوعیت پیدا می‌کند که غبار ابهام را از چهره آن می‌زداید تا بتواند به سیاست‌های مشخصی جهت اداره انسان تبدیل شود. از این حیث، دکترین حاکم، ضرورتاً یک ایدئولوژی و مجموعه‌ای سازمان‌یافته درباره بهترین شیوه زندگی مردم و درباره مناسب‌ترین ترتیبات نهادی برای جوامعشان می‌باشد؛ بنابراین، دکترین (قاعدة القواعد) تبیین و تشریح قواعد ذاتی حاکم بر خلقت، طبیعت و قواعد ذاتی حاکم بر اعمال موجودات، به‌ویژه بشر است. تبیین این قواعد مبتنی بر، «باید» برای جامعه‌سازی الزامی است.لذا موضوع این رویکرد، مطالعه جامعه از حیث قواعد ذاتی حاکم بر خلقت، طبیعت و رفتار موجودات و انسان است [۳].

دکترین، عبارت است از یک نیروی واسطه‌ای میان فلسفه و سیاست [۳] فلسفه همواره در ابتدا می‌آید و دکترین از آن ناشی می‌شود. سیاست نیز به‌نوبه خود از دکترین نشئت می‌گیرد [۳] در حقیقت دکترین، فلسفه را که اغلب ابهام‌آلود و نظری است، می‌گیرد و آن را عملیاتی می‌کند تا از دل آن، سیاست‌هایی خاص

[۱] الف-فضای مجازی: فضای مجازی، امتزاجی از فضای حقیقی می‌باشد که به ابزاری جهت بسط و تحکیم حاکمیت ملی در مناسبات جهانی و کشوری مبدل شده است. ب-دکترین: اصول و قواعدی است که در یک علم خاص و به‌منظور هدایت‌گری و کاربست عملی به کار می‌رود. ج-دکترین سایبری دفاعی امنیتی جمهوری اسلامی ایران: به‌عنوان راهنمای نظری و عملی راهبردی نیروهای دفاعی امنیتی (در شرایط امنیتی صلح، بحران و جنگ)، فلسفه حاکمیتی واحد برای عملیات نرم و سخت و حکمرانی روابط بین‌المللی سایبری؛ مورداستفاده قرار می‌گیرد [۱۰].



شکل ۱: تبیین الگوی سیاست‌گذاری بر مبنای رهیافت دکترینی [۳]

بیرون بیاید [۳]. به تعبیر دیگر، دکترین تعیین‌کننده سیاست است و یک سیاست عمومی، عبارت است از اجرای زیرمجموعه‌ای از یک دکترین حاکم [۳] و تمامی سیاست‌های عمومی، ریشه در یک دکترین مشخص دارند آن‌ها برای تبیین الگوی سیاست‌گذاری بر مبنای رهیافت دکترینی نمودار زیر را ارائه می‌نمایند و با تأکید بر کاربردی بودن این الگو می‌گویند: نکته مفید در خصوص این‌گونه تصویرسازی ما این است که آن‌ها را می‌توان در مورد همه انواع سیاست‌ها به کار برد.

تعریف دکترین از منظر برخی سازمان‌های حقوقی به شرح زیر می باشد:

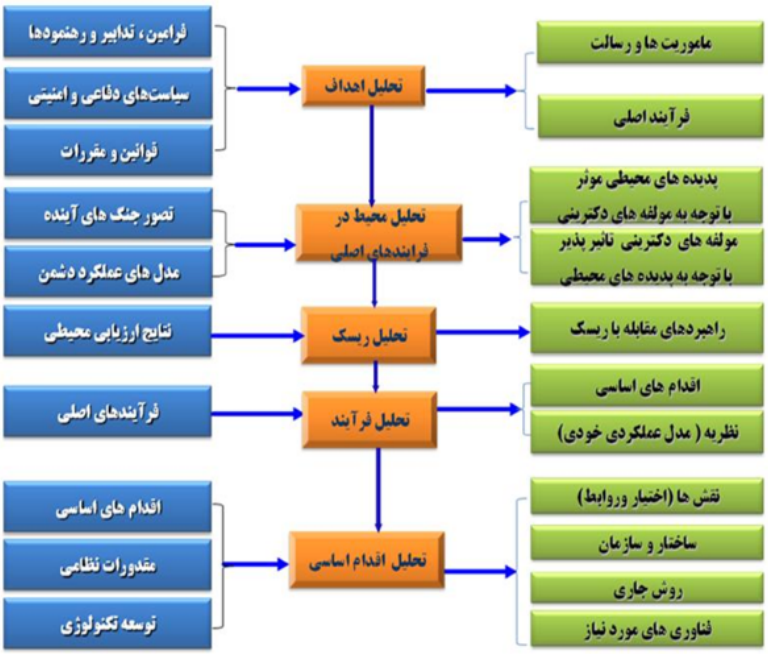
ستاد کل نیروهای مسلح: مجموعه‌ای از قواعد نسبتاً پایدار و کاربردی که چگونگی انجام مأموریت و اجرای عملیات را ترسیم می‌کند و مبنا و راهنمای برنامه‌ریزی‌های اقدامات است. رهنامه (دکترین) ایده‌ای است کلی معطوف به راه و روش برای رسیدن به اهداف. معمولاً دکترین متأثر از چهار مقوله است: ۱. نوع سازمان و مأموریت آن. ۲. محیط (به‌ویژه تهدیدات) ۳. قدرت نظامی و دفاعی ۴. علم و فناوری [۴].

فرهنگ اصطلاحات نظامی وزارت دفاع آمریکا: اصول بنیادینی که نیروهای نظامی و وابستگان آن‌ها توسط آن، فعالیت‌های خود را در راستای تأمین اهداف ملی هدایت می‌کنند(۲۰۲۰).

فرهنگ اصطلاحات دفاعی ناتو: اصول بنیادینی که نیروها و فعالیت‌هایشان را جهت نیل به اهداف هدایت می‌کند. این اصول دستوری بوده لیکن اجرای آن‌ها قضاوتی (منوط به رأی) می‌باشند (۲۰۱۹).

۲.۲ ماهیت‌شناسی دکترین

دکترین شیوه‌ای است که می‌گوید چگونه باید برای پیروزی بجنگیم و شامل سه عنصر اساسی نظریه، فرهنگ و اقتدارمی‌شود. اول از همه، دکترین باید برمبنای تلقیات از کار انجام‌شده و چیزی که باعث پیروزی در آن محیط می‌شود، قرار گیرد. به‌عبارت دیگر یک دکترین به یک عنصر نظریه نیاز دارد.باید بدانیم که چرا چیزی صادق است تا اثر آن را بگذارد. به‌علاوه این دکترین است که دلیل آن را توضیح می‌دهد. ثانیاً یک دکترین باید عوامل فرهنگی را موردتوجه قرار دهد.سرانجام، دکترین به‌نوعی اقتدار رسمی نیاز دارد چون در غیر این صورت اثر یکپارچه‌سازی و «هماهنگ‌کننده فکر» را نخواهد داشت. متعادل کردن سه عنصر فوق، یعنی نظریه، فرهنگ و اقتدار، می‌تواند به طرق مختلف انجام شود و با این کار می‌توان سه نوع دکترین ایده‌آل را تولید کرد: دکترین به‌عنوان ابزاری برای فرماندهی، تغییر و آموزش [۱۱].



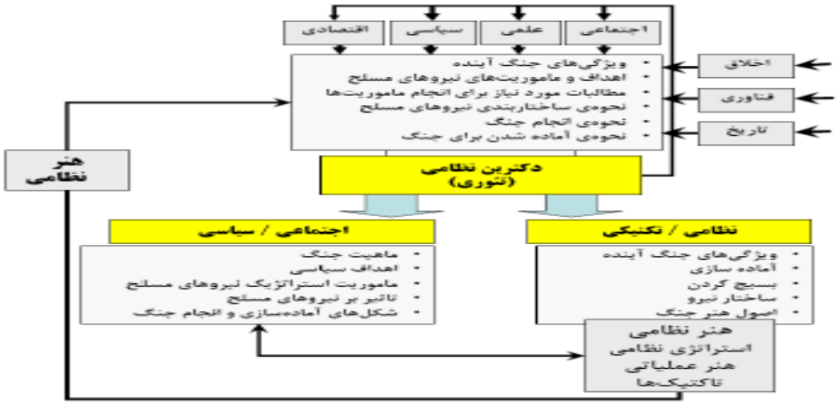
شکل ۲: فرآیند پنج مرحله‌ای تدوین دکترین [۵]

۳ برخی از مدل‌های تدوین دکترین

طبق بررسی‌های به‌عمل آمده تاکنون جهت تدوین دکترین سایبری در ج.ا.ا. روشی تدوین شده‌ای وجود ندارد، لیکن به‌صورت کلی جهت تدوین دکترین چندین الگو پیشنهاد شده است که در زیر به‌صورت مختصر مرور می‌گردد.

مدل سیستمی: این مدل توسط هیأت عالی آئین‌نامه‌های ن.م. ارائه شده است. در این مدل، خلق یا تجدید نظر در یک دکترین جدید در طی پنج مرحله به شرح ذیل انجام می‌پذیرد. از ویژگی‌های منحصر به فرد این مدل آن است که باعث می‌گردد تا فعالیت‌های انجام‌شده در تیم‌های تدوین‌کننده دکترین از چارچوب واحدی پیروی کرده و ضمن ایجاد یکنواختی، امکان ارزیابی را برای اطمینان از توجه همه‌جانبه به اجزای دکترین فراهم‌نماید [۵].

مدل دکترین نظامی: دکتر دانش آشتیانی در مقاله «اصول و روش تدوین دکترین نظامی»، یک روش پنج مرحله‌ای برای تدوین دکترین نظامی معرفی نموده‌اند. مرحله اول: شناسایی مناقشه (جنگ) و ماهیت آن؛ مرحله دوم: بررسی نقطه نظرات دشمن (نیات دشمن)؛ مرحله سوم: توسعه راهبرد ملی؛ مرحله چهارم: توسعه راهبرد نظامی (ملّی)؛ مرحله پنجم: توسعه و تدوین دکترین نظامی (ملّی) [۶].



شکل ۳: مدل تدوین دکترین در روسیه [۷]

مدل تدوین دکترین در روسیه: عبدالرسول دیو سالار در مقاله خود به تشریح روش تدوین دکترین در روسیه می پردازد و بیان می کند که مفهوم دکترین در ادبیات شرق و غرب از تفاوت قابل توجهی برخوردار است. در ادبیات شرقی دکترین نقش محوری در انتقال دیدگاه ها و باورهای رسمی نسبت به جنگ آینده ومحیط امنیتی پیش رو دارد. در حالی که در غرب دکترین شعور ناپیدای حاکم بر بکارگیری نیروهای مسلح در صحنه نبرد تعبیر می شود که بر پایه مفاهیم عملیاتی شکل گرفته و ارتباط میان فناوری، ساختار، تئوری و تجربه رزمی را برقرار می‌سازد در شرق دکترین برداشت مشترکی از مطالبات دفاعی ملی است [۷].

مدل دکترین جنگ سایبری: لچ جی. جانشکی و آندره ام. کلاریک در مقاله ای با عنوان «ایجاد دکترین جنگ سایبری» مدلی را جهت تدوین دکترین جنگ سایبری پیشنهاد می دهند.به طور خلاصه، چارچوب پیشنهادی برای توسعه دکترین جنگ سایبری ملی مبتنی بر چندین اصل اساسی است. اولین مورد این است که چنین فرآیندی در حیطه اختیارات دولت انجام می‌شود، هم در مورد شروع روند دکترین جنگ سایبری و هم در مورد پذیرش نهایی آن. توسعه دکترین جنگ سایبری باید به متخصصان غیرنظامی دولت، کارکنان حوزه دفاعی-امنیتی و سازمان‌های حرفه‌ای مرتبط با فناوری اطلاعات واگذار شود. پیشنهادهای نهایی به شورای امنیت در سطح ملی (یا نهاد دیگری با مسئولیت‌های مشابه) ارائه شود و در نهایت توسط رئیس دولت پذیرفته می‌شود. در نهایت دکترین جنگ سایبری در معرض عموم قرار می‌گیرد [۱۲].

۴ مفهوم‌شناسی دکترین سایبری در حوزه دفاعی امنیتی

موضوع تدوین دکترین سایبری یک موضوع فرا سازمانی و ملی است که تدوین آن مستلزم شناخت مؤلفه‌های مرتبط با آن در سیاست‌های ابلاغی، قانون اساسی و اسناد بالادستی این حوزه است. سایبرنتیک واژه پرکاربرد حوزه کنترل و ارتباطات در نیمه دوّم قرن بیستم میلادی است. این واژه از لغت یونانی Κυβερνήτης به

معنای سکان‌دار والی اخذ شده است[۲]. سکان‌دار در ناوبری کشتی کسی است که با رصد سرعت و جهت وزش باد و تأثیر آن بر امواج دریا و با در نظر گرفتن سمت و جهت مقصد، سکان کشتی را به چپ و راست می‌چرخاند.سایبرنتیک حضور حسگرها، اطلاعات، تصمیم‌سازی و تصمیم‌گیری و اعمال قدرت در ناوبری است و عدم وجود هر یك ناوبری را دچار مشکل خواهد کرد [۸]. برخی از تعاریف فضای سایبر عبارتند از:

شورای عالی فضای مجازی: فضای مجازی جمهوری اسلامی ایران فضایی در امتداد فضای واقعی، سالم، ایمن، مفید، پیشران پیشرفت سایر حوزه‌ها است (۱۳۹۷).

پیمان آتلانتیک شمالی (ناتو): فضای مجازی مجموعه‌ای وابسته به زمان از سیستم‌های اطلاعاتی به‌هم‌پیوسته و کاربران انسانی است که با این سیستم‌ها در تعامل هستند (۲۰۱۷).

تعریف مشترك روسیه و آمریکا: یک رسانه الکترونیکی که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌شوند (۲۰۱۴).

نیروهای مسلّح عملیات فضای مجازی و جنگ الکترونیکی را در محیط اطلاعاتی انجام می‌دهند. محیط اطلاعاتی مجموعه‌ای از افراد، سازمان‌ها و سیستم‌هایی تشکیل‌شده است که اطلاعات را جمع‌آوری، پردازش، انتشار یا طبق آن عمل می‌کنند. سهولت دسترسی به شبکه‌های فنی باعث کمک به اشتراک‌گذاری اطلاعات می‌شود و جنبه‌های اجتماعی محیط اطلاعاتی را تقویت می‌کند.ابعاد محیط اطلاعاتی عبارت‌اند از فیزیکی، اطلاعاتی و شناختی. عملیات اطلاعاتی، چه در داخل و چه در خارج از فضای مجازی، می‌تواند بر روی عملیات دوستانه، خنثی و تهدیدی در فضای مجازی تأثیر بگذارد [۱۳].

قدرت بازدارندگی: هر کشوری که بخواهد تحت سلطه نباشد، برای حفظ استقلال و هویت باید توان مقابله با حملات دشمنان را داشته باشد و بتواند به بهترین شکل از خود دفاع کند. جمهوری اسلامی ایران از ابتدای تشکیل با انواع گوناگونی از توطئه‌های مستکبرین روبه‌رو بوده و تهدید به حمله نظامی یکی از گزینه‌های روی میز دشمنان است. با توجه به این چالش، تدارک نیروهای مسلّح مقتدری که از حداکثر توانایی برخوردار بوده و توان مقاومت در برابر انواع دشمنی‌ها را داشته باشند، ضروری است.این همان چیزی است که در ادبیات سیاسی از آن به‌عنوان قدرت بازدارندگی تعبیر می‌شود و یکی از مهم‌ترین اهداف قرآنی نظام اسلامی است [۱].

ده استنباط از دیدگاه‌های مقام معظم رهبری (مد ظله العالی): ۱- عدم انکار فضای مجازی در انقلاب اسلامی. ۲- فضای مجازی پایه‌گذار تمدن اسلامی. ۳- واقعیت فضای مجازی در مقابل رویکرد دوجهانی. ۴- رویکرد مبتکرانه و فرصت‌آفرین و هوشمند در مواجهه با فضای مجازی. ۵- فضای مجازی ابزار بسط حاکمیت ملی در مناسبات جهانی و کشوری. ۶- چالش دوقطبی‌سازی سیاسی کاذب در توسعه کشور. ۷- چالش تسلط کمپانی‌های بزرگ تحت سلطه آمریکا. ۸- چالش شکاف توسعه در مقایسه با روند

[۲] لفظ Governor به‌معنای فرماندار با سایبرنتیک هم‌ریشه است.

پیشرفت و شتاب فناوری. ۹- توان و ظرفیت زیرساختی بالقوه (مردم - نخبگان - فناوری - ساختار- اقتصاد). ۱۰- ضرورت تدوین نقشه راه حکمرانی در فضای مجازی [۹].

قانون اساسی: برخی از اصول مهم قانون اساسی عبارتند از: اصل(۹) اصول تفکیک‌ناپذیر: آزادی، استقلال، وحدت، تمامیت اراضی کشور

اصل(۲۶) اصول ج. ا. ایران: استقلال، آزادی، وحدت ملی، موازین اسلامی

اصل(۱۷۶) اصول شورای عالی امنیت ملی: تأمین منافع ملی، پاسداری از انقلاب اسلامی، تمامیت ارضی، حاکمیت ملی

اصل(۱۵۲) سیاست خارجی ج.ا.ا: نفی هرگونه سلطهجویی و سلطهپذیری؛ حفظ استقلال همه‌جانبه و تمامیت ارضی کشور؛ دفاع از حقوق همه مسلمانان؛ عدم تعهد در برابر قدرتهای سلطهگر؛

برخی از مهم ترین اسناد بالادستی در مورد دکترین سایبری جمهوری ا. ایران در حوزه دفاعی و امنیتی به شرح زیر می‌باشند. علاوه بر اسناد یادشده فوق، سایر اسناد سیاستی که دارای ماهیت دفاعی امنیتی و فناوری اطلاعات می‌باشند، به‌طور کامل مدنظر قرار می‌گیرند.

- سند چشم‌انداز ۱۴۰۴ ساله (۱۳۸۲): ایران کشوری است: امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه و پیوستگی مردم و حکومت؛ آزادی‌های مشروع، حفظ کرامت وحقوق انسان‌ها و بهره‌مند از امنیت اجتماعی و قضایی؛ الهام‌بخش، فعال و مؤثر در جهان اسلام؛ دارای تعامل سازنده و مؤثر با جهان بر اساس اصول عزت، حکمت و مصلحت.
- حکم مقام معظم رهبری (مد ظله‌العالی) دوره دوّم شورای عالی فضای مجازی (۱۳۹۴): ۳-ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی و برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه. ۱۰- تدوین و تصویب نظام‌های امنیتی، حقوقی، قضایی و انتظامی موردنیاز در فضای مجازی.
- گام دوّم انقلاب۱۳۹۷: توصیه‌هایی اساسی به‌منظور جهاد بزرگ برای ساختن ایران ا. بزرگ (ایجاد تمدّن عظیم اسلامی هدف نهایی جمهوری اسلامی ایران، امید و نگاه خوش‌بینانه به آینده، برپا کردن تمدّن اسلامی منتها با روح اسلامی و معنویّت)

۵ نتیجه‌گیری

پس از بررسی مدل‌های مختلف تدوین دکترین در دنیا، نظریه‌های دفاعی امنیتی جمهوری اسلامی ایران و ویژگی‌های فضای سایبر، محققین به یک مدل فرآیندی جهت تدوین دکترین سایبری ج.ا.ا به شرح زیر دست یافتند. در ادامه با برگزاری جلسه گروه کانونی، متشکل از تعدادی از خبرگان در این حوزه مدل به نقد و بررسی گذاشته شد و اشکالات مدل احصاء و تصحیح گردید. سپس مدل تصحیح شده در قالب پرسش‌نامه

شکل ۴: مدل فرآیندی تدوین دکترین سایبری ج.ا.ا

نیمه ساختاریافته به خبرگان ارائه و مجدداً نظرات جمع‌آوری گردید. در راستای اعتبارسنجی مدل، نسبت به تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی اقدام گردید. با اعتبارسنجی دکترین به‌دست آمده ، روایی مدل تدوین‌شده نیز احصاء گردید [۱۰].

مراجع

[۱] امام خامنه‌ای (مدظله‌العالی)، مجموعه بیانات، قابل‌دسترسی در: www.farsi.khamenei.ir

[۲] خسروپناه، عبدالحسین و یزدانی‌فر، صالحه (زمستان ۱۳۹۵)، نظام مدیریتی فقه و فرآیند سیاست‌گذاری و طرح‌ریزی، فصلنامه راهبرد فرهنگ، دوره نهم، شماره ۳۶، صفحات: ۴۱-۷.

[۳] بوریک، کریستوفرپی، شافریتز، جی.ام (۱۳۹۰)، سیاست‌گذاری عمومی در ایالات‌متحده آمریکا، ترجمه حمیدرضا ملک محمدی. تهران: دانشگاه امام صادق.

[۴] ستاد کل نیروهای مسلّح ج.ا.ایران (۱۳۸۹)، اصطلاحات و واژگان.

[۵] ثروتی، محسن و همکاران (۱۳۹۱)، راهنمای آموزشی تدوین دکترین، تهران، انتشارات دبیرخانه هیئت عالی آئین‌نامه‌های نیروهای مسلح.

[۶] دانش آشتیانی، محمدباقر (۱۳۸۸)، اصول و روش تدوین دکترین نظامی. فصلنامه نظم و امنیت انتظامی، شماره سوم سال دوم.

[۷] مؤسسه آموزشی و تحقیقات صنایع دفاعی (۱۳۸۶)، ارزیابی ابعاد گوناگون دکترین‌های امنیتی- دفاعی روسیه، تهران.

[۸] کیانخواه، احسان (۱۳۹۷)، تبیین ماهیت و مؤلفه‌های فضای سایبر بر اساس تفکر اسلامی، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاع ملی.

[۹] ولوی، محمدرضا (۱۳۹۲)، طرح تحقیق دفاع سایبری آینده.

[۱۰] مرادی، محمدرضا (۱۴۰۱)، تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاع ملی.

[11] Harold Hoiback (2015), The Anatomy of Doctrine and Ways to Keep It Fit , Journal of Strategic Studies.

[12] M. Colarik, Andrew, Janczewski, Lech (2012), Establishing Cyber Warfare Doctrine, Journal of Strategic Security, Volume 5, Number 1 Volume 5, No. 1: Spring 2012.

[13] Department of the Army (2017), FM 3-12, cyberspace and electronic warfare operation. Available at: http://www.apd.army.mil