فصلنامه تهدیدپژوهی
سال اول، شماره دوم
تابستان ۱۴۰۲
صص: ۳۰ – ۱

مرکز مطالعات و پژوهش‌های اطلاعاتی

الزامات و بایسته‌های تدوین دکترین سایبری دفاعی امنیتی ج.ا.ایران

محمدرضا مرادی*[۱]، متین مرادی[۲]

تاریخ دریافت: ۱۴۰۱/۱۲/۱۵ **تاریخ پذیرش: ۱۴۰۲/۰۲/۲۵**

چکیده

فضای سایبری باعث تأثیر در مفاهیم پایه‌ای جغرافیای سیاسی همچون مفهوم ملت، حکومت، مرز و غیره شده است. امنیت ملی هم به‌شدت تحت تأثیر فضای سایبر قرارگرفته است که باید تحولات آن در زیست‌بوم سایبری مورد تجزیه‌وتحلیل اساسی قرار گیرد. بی‌توجهی و نادیده گرفتن اهمیت و ضرورت تدوین خط‌مشی‌ها و روش‌های اصول منطقی دفاعی و امنیتی، امنیت ملی را در معرض خطر قرار می‌دهد. الزام به تدوین اسناد بالادستی در حوزه سایبری: علاوه بر تأکید در بیانات مقام معظم رهبری (مدظله‌العالی)، در سند سیاست‌های کلی نظام در بخش "امنیت فضای تولید و تبادل اطلاعات" نیز مشاهده می شود. یکی از اسناد حائز اهمیت در این حوزه که باعث ایجاد بازدارندگی مقتدرانه، مقابله با حملات و کمک به جلوگیری از درگیری‌های آینده در حوزه سایبر، دکترین است. این مقاله بر آن است به تبیین مبانی نظری ازجمله مبانی تدوین، منابع ورودی و سؤالات اساسی که دکترین سایبری باید به آن پاسخ بدهد و در جهت تدوین دکترین سایبری به آن نیاز است پاسخ بدهد و ضمن برر سی منابع موجود در تدوین دکترین مبتنی بر سه اصل چیستی، چرایی و چگونگی با دیدگاه عمدتاً شرقی، روش‌های تدوین دکترین علی‌الخصوص در حوزه سایبری را مداقه قرار دهد. رویکرد این تحقیق کیفی بوده و از روش گردآوری کتابخانه‌ای و ابزار فیش‌برداری اسناد بالادستی، نشریات، مقالات تخصصی استفاده نموده است. با توجه به ویژگی‌های خاص فضای سایبر و پویایی فراوان آن روش تدوین دکترین سایبری علاوه بر اشتراکات با سایر حوزه‌ها از ویژگی‌های منحصربه‌فردی نیز برخوردار است. معرفی چند الگوی تدوین دکترین و یک الگوی تدوین دکترین سایبری از نتایج این مقاله است.

واژگان کلیدی: دکترین، فضای سایبری، دفاعی– امنیتی

استناد: مرادی، محمدرضا؛ مرادی، متین (۱۴۰۲). الزامات و بایسته‌های تدوین دکترین سایبری دفاعی امنیتی ج.ا.ایران. *فصلنامه تهدیدپژوهی ۱(۲). ۱–۳۰*

---

۱. دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی(نویسنده مسئول)
۲. دانشجوی مهندسی کامپیوتر دانشگاه شاهد

Center for Intelligence Studies and Research

Quarterly Journal of Threat Studies
Volume 1, Issue2
Summer 2023

PP 1 - 30

Requirements and Requirements for Developing the Cyber Defense and Security Doctrine of the Republic of Iran

Mohammad Reza Moradi*[1], Matin Moradi[2]

Received: 2023/03/06 **Accept:2023/05/15**

Abstract

Cyberspace has affected the basic concepts of political geography, such as the concept of nation, government, border, etc. National security has also been greatly affected by cyberspace, and its developments in the cyber ecosystem must be fundamentally analyzed. Ignoring and ignoring the importance and necessity of formulating policies and methods of logical defense and security principles puts national security at risk. . The requirement to formulate upstream documents in the cyber domain: In addition to the emphasis in the statements of the Supreme Leader (Ayatollah Ali Khamenei), it is also seen in the document of the general policies of the system in the section "Security of the production space and information exchange." One of the important documents in this area that creates authoritative deterrence, confronts attacks, and helps prevent future conflicts in the cyber domain is the doctrine. This article aims to explain the theoretical foundations, including the principles of formulation, input sources, and basic questions that the cyber doctrine must answer and that are needed in order to formulate the cyber doctrine. While examining the resources available in the formulation of the doctrine based on the three principles of what, why, and how from a mainly Eastern perspective, it also examines the methods of formulating the doctrine, especially in the cyber domain. The approach of this research is qualitative and uses the library collection method and the tool of document retrieval of upstream documents, publications, and specialized articles. Considering the special characteristics of cyberspace and its great dynamism, the method of formulating cyber doctrine has unique features in addition to commonalities with other fields. Introducing several doctrine formulation patterns and a cyber doctrine formulation pattern is one of the results of this article.

Keywords: Doctrine, Cyberspace, Defense-Security

Citation: Moradi, Mohammad Reza; Moradi, Matin (1402). Requirements and Requirements for Developing the Cyber-Defense-Security Doctrine of the Republic of Iran. *Quarterly Journal of Threat Studies 1(2). 1-30.*

1. PhD in Strategic Cyberspace Management, National Defense University (Responsible author)

2. Computer Engineering Student, Shahed University

مقدمه

پدید نوظهور فضای مجازی تأثیر شگرفی بر سبک زندگی انسان در عصر جدید داشته است. این پدیده به‌عنوان یک قدرت نرم فوق‌العاده، در جنبه‌های مختلف ازجمله فرهنگ، سیاست، اقتصاد، ایمان، اعتقادات دینی و اخلاقیات، تأثیرگذاری خیره‌کننده‌ای دارد (بیانات مقام معظم رهبری (مدظله‌العالی)، شانزدهم شهریور ۱۳۹۴).

بنیاد هریتیج ذیل پروژه ۲۰۲۵ اقدام به تدوین و انتشارسندی[1] با عنوان "حکم (دستور) برای رهبری: عهد محافظه کاران" نموده است. نمای کلی پروژه ۲۰۲۵ درخصوص ایران نشانگر اتخاذ آرایش تهاجمی‌تر در دولت جدید ترامپ است (بنیاد هریتیج،۲۰۲۵).

امروزه، دیگر نمی‌توان فضای سایبر را صرفاً به عنوان یک بستر برای ارتباطات و تبادل اطلاعات در نظر گرفت. این فضا به عرصه‌ای برای رقابت، منازعه و حتی جنگ تبدیل شده است. کشورها و سازمان‌های مختلف، اعم از دولتی و غیردولتی، از فضای سایبر برای پیشبرد اهداف خود، اعم از سیاسی، اقتصادی و نظامی، بهره می‌برند. در این میان، تهدیدات سایبری، از جمله جاسوسی، خرابکاری، سرقت اطلاعات و حملات سایبری به زیرساخت‌های حیاتی، به طور چشمگیری افزایش یافته است. به علاوه بسیاری از کشورها و سازمان‌ها، از جمله ایالات متحده آمریکا (که وزارت دفاع آن به طور رسمی فضای سایبری را به عنوان عرصه پنجم جنگ تعریف کرده است)، ناتو (که در سال ۲۰۱۶ به طور رسمی فضای سایبری را به عنوان عرصه عملیاتی خود تعریف کرد)، بریتانیا، چین و روسیه، فضای سایبری را به عنوان عرصه پنجم جنگ در کنار زمین، دریا،

1- Mandate for Leadership: The Conservative Promise

هوا و فضـــا تعریف کرده‌اند و بر اهمیت آن در راهبردهای نظامی و دفاعی خود تأکید دارند.

جمهوری اســـلامی ایران نیز به عنوان کشـــوری که در معرض تهدیدات مختلف ســـایبری قرار دارد، نیازمند تدوین یک دکترین ســـایبری دفاعی امنیتی جامع و کارآمد اســـت. چنین دکترینی باید با در نظر گرفتن ویژگی‌های خاص کشـــور، از جمله موقعیت جغرافیایی، ساختار سیا سی و اجتماعی، و توانمندی‌های دفاعی، چارچوبی جامع برای سیا ست‌ها، راهبردها و اقدامات دفاعی و امنیتی در فضای سایبر ارائه دهد.

در سند راهبردی جمهوری اسلامی ایران در فضای مجازی (مصوب سال ۱۴۰۱) که شورای عالی فضای مجازی منتشر نموده فضای مجازی جمهوری اسلامی ایران در افق ۱۴۱۰ فضـــایی در امتداد فضـــای واقعی، ســـالم، ایمن، مفید، پیشـــران پیشرفت سایر حوزه‌ها است.

با گسترده و امنیتی شدن فضای سایبر و افزایش ذینفعان در بخش‌های حاکمیتی، خصوصی و سازمان‌های تخصصی، این فضا بیش‌ازپیش نیازمند قانونمند شدن اســـت. بی‌توجهی و نادیده گرفتن اهمیت و ضـــرورت تدوین خط‌مشـــی‌ها و روش‌های اصـــول منطقی دفاعی و امنیتی، امنیت ملی را در معرض خطر قرار می دهد.

الزام به تهیه و تدوین اسناد بالادستی در حوزه سایبری، علاوه بر تأکید مقام معظم رهبری (مدظله‌العالی) در حکم اعضای شورای عالی فضای مجازی در سال ۱۳۹۴، در سند "امنیت فضای تولید و تبادل اطلاعات" نیز مشاهده می‌گردد. یکی از مهم‌ترین اسناد بالادستی در این حوزه که می‌تواند به‌عنوان یک عامل انسجام بخش موجب ایجاد وحدت رویه گردد، دکترین سایبری است.

بیان مسئله

آسیب‌های وارده به ج.ا.ایران در حوزه‌های دفاعی و امنیتی سایبری در اشکال سخت، نیمه سخت و نرم متجلی شده و سال‌به سال نیز وجوه کاملاً جدیدی می‌یابد. نقطه کانونی این حوادث به مخاطره افکندن امنیت ملی جمهوری اسلامی ایران است. البته ج. ا.ایران نیز در جهت مقابله با اثرات مخرب این فضا به یک رویکرد فعال بازدارنده روی آورده است.

در سال ۱۳۹۰ شورای عالی فضای مجازی به تشخیص مقام معظم رهبری (مدظله‌العالی) به‌عنوان بالاترین نهاد حاکمیتی در شرایطی شکل گرفت که در فضای مجازی کشور ناهماهنگی بین دستگاه‌های اجرایی وجود داشت.

در شرایط کنونی، نهادهای دفاعی امنیتی که وظیفه اصلی دفاع سایبری در کشور و برقراری امنیت در این فضا را بر عهده‌دارند به دلیل گستردگی و فراگیر شدن فضای مجازی دارای شرح وظایف متنوع و بعضاً مشابهی در حوزه فضای سایبری گردیده‌اند لیکن دارای برداشت‌های یکسان، تعاریف استاندارد بومی در مفاهیم پایه و... نمی‌باشند از سوی دیگر تعدد ذینفعان و متولیان در این حوزه و همچنین نبود جهت‌گیری واحد و مواضع اصولی موجب گردیده مسئولین و فرماندهان ضمن انجام اقدامات سلیقه‌ای و حرکات موازی، ناخواسته مسبب پدید آمدن آسیب و ایجاد چالش در فرآیند دفاعی امنیتی سایبری کشور گردند. (مرادی و همکاران ،۱۴۰۱)

موارد یادشده فوق موجب عدم انسجام کافی، یکپارچگی و وحدت رویه در بهره‌برداری از فرصت‌ها و پاسخگویی به تهدیدات فضای سایبر می‌گردد. از سوی دیگر عضویت برخی از نهادهای دفاعی امنیتی در شورای عالی فضای مجازی رافع نیازمندی‌های این حوزه نیست.

در راستای برطرف نمودن چالش مذکور با بهره‌مندی از اسناد بالادستی، دکترین می تواند به‌عنوان راهنمای مکتوب جهت‌گیری یکپارچه اقدامات و پاسخی به دغدغه‌های ذکرشده فوق و راهکاری برای اجماع و اتفاق‌نظر در حوزه دفاعی و امنیتی فضای سایبر باشد. به این دلیل که دکترین بیان می‌کند که چگونه می‌توان کاری را به بهترین شکل ممکن انجام داد و به نسل‌های بعدی منتقل‌نمود.

مدل‌ها و فرایند طراحی دکترین در کشورهای مختلف متفاوت است و رویکرد هر کشور نیز به مقتضیات همان کشور برمی‌گردد. بررسی‌های نشان می‌دهد که الگو و روش مدون و بومی جهت تدوین دکترین سایبری در ج.ا.ایران وجود ندارد. از سوی دیگر تهیه و تائید یک الگو نیازمند تبیین برخی از الزامات و مطالعات اولیه است که به‌صورت منسجم و منتشرشده یافت نگردید.

با عنایت به موارد یادشده، می‌توان مسئله اساسی این تحقیق را فقدان تبیین مبانی نظری ازجمله مبانی تدوین، منابع ورودی و سؤالات اساسی که دکترین سایبری باید به آن پاسخ بدهد است.

مفاهیم و اصطلاحات

در این بخش، مفاهیم فضای سایبر، دکترین، دفاع و امنیت تبیین می‌شود.

۱- 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 (مرادی و همکاران،۱۴۰۱).

۲- دکترین: ازنظر لغوی، دکترین در فرهنگ لغات فارسی با واژه‌هایی مانند مسلک، عقیده، رأی، نظریه و فکر (فرهنگ عمید، ص: ۱۱۳۴) مترادف است. به معنای اصول بنیادین، باورها و چارچوب های نظری، دیدگاه، الگو، خط‌مشی، چگونگی عمل، راهنما و روش است. (ثروتی، مظلوم؛۱۳۹۱) در

برخی منابع نیز از واژه "رهنامه" به‌عنوان معادل فارسی دکترین استفاده‌شده و این تعریف برای آن ارائه‌شـده اسـت: رهنامه مجموعه‌ای از اصـول و قواعد اساسی است که به‌واسطه نظر خبرگان مرتبط با اولویت‌بندی مناسب کنار هم قرار می‌گیرند (افشـردی و همکاران، ۱۳۹۶). اصـول و قواعدی اسـت که در یک علم خاص و به‌منظور هدایت‌گری و کاربست عملی به کار می‌رود(مرادی و همکاران،۱۴۰۱).

۳- دکترین (حوزه امنیت ملی): شـامل اصـول راهنما برای کاربرد مؤلفه‌های قدرت ملی اسـت که با توصـیف شـرایط محیطی، روش‌ها و وضـعیت به‌کارگیری این مؤلفه‌ها را تعیین می‌نماید (معمار زاده و پورشاسب، ۱۳۸۶).

۴- دکترین سایبری: به‌عنوان یک راهنما برای نیروهای دفاعی در زمان جنگ، فلسـفه حاکمیتی واحد برای عملیات نظامی، محافظت از زیرسـاخت‌های غیرنظامی و حکمرانی روابط بین‌المللی سـایبری؛ و به‌عنوان یک بازدارنده برای دشمنان آینده مورداستفاده قرارمی گیرد.(جانشسکی و کلاریک،۲۰۱۲). دکترین سـایبری، چارچوب راهبردی جامعی اسـت که نحوه سـازماندهی، استفاده و یکپارچه سازی قابلیت‌های سایبری یک کشور یا سازمان را برای حفاظت از زیرساخت‌های دیجیتال حیاتی، بازدارندگی از دشمنان و در مواقع ضـروری اجرای عملیـات‌هـای تهـاجمی در حوزه دیجیتـال تشـریح می‌کند.(راهبرد سایبری وزارت دفاع ایالات متحده،۲۰۱۸)

۵- دکترین سـایبری دفاعی امنیتی جمهوری اسـلامی ایران: به‌عنوان راهنمای نظری و عملی راهبردی نیروهای دفاعی امنیتی (در شـرایط امنیتی صـلح، بحران و جنگ)، فلسـفه حاکمیتی واحد برای عملیات نرم و سـخت و حکمرانی روابط بین‌المللی سـایبری؛ مورداسـتفاده قرار می‌گیرد. (مرادی و همکاران،۱۴۰۱).

اهمیت و ضرورت انجام تحقیق

در دنیای پرتلاطم و پیچیده امروز، فقدان دکترین سایبری دفاعی امنیتی جامع و کارآمد برای ج.ا.ایران، چالش‌های بنیادینی را در مسیر حفظ امنیت ملی و منافع حیاتی کشور ایجاد می‌کند و کشور در برابر تهدیدات گوناگون سایبری به شدت آسیب‌پذیر خواهد بود و بدون نقشه راه مشخص، هماهنگی و انسجام لازم بین دستگاه‌های مسئول در حوزه سایبر مختل شده و از ظرفیت‌های موجود به نحو مطلوب استفاده نخواهد شد و علاوه بر این، توان بازدارندگی کشور را در این حوزه تضعیف کرده و دشمنان را به انجام حملات سایبری تشویق می‌کند و در چنین شرایطی، کشور در برابر حملات سایبری غافلگیر شده و واکنش مؤثر و به‌موقع در برابر آنها با دشواری‌های فراوانی روبرو می‌شود و همچنین، ارزیابی و بهبود مستمر وضعیت امنیت سایبری کشور نیز بدون وجود یک دکترین مشخص، با چالش‌های جدی روبرو خواهد شد.

در مقابل، درصورت تدوین دکترین سایبری دفاعی با تعیین اصول و قواعد حاکم بر فضای سایبر، چارچوبی منسجم و مدون برای فعالیت‌های سایبری در سطح ملی فراهم می‌کند و در پرتو چنین سند راهبردی، کشور قادر خواهد بود تا با شناسایی دقیق تهدیدات و آسیب‌پذیری‌ها، ظرفیت‌های دفاعی خود را به طور هدفمند توسعه داده و از آنها به نحو مؤثر بهره‌برداری کند و علاوه بر این، دکترین سایبری، با ایجاد هماهنگی و انسجام بین دستگاه‌های مختلف، از موازی‌کاری و تداخل وظایف جلوگیری کرده و امکان استفاده بهینه از منابع و توانمندی‌های کشور را فراهم می‌سازد و از سوی دیگر، تدوین دکترین سایبری، با شفاف‌سازی مواضع و توانمندی‌های کشور در حوزه سایبر، نقش مهمی در ایجاد بازدارندگی در برابر تهدیدات سایبری ایفا می‌کند و از بروز جنگ‌های سایبری پرهزینه پیشگیری می‌کند.

اهداف تحقیق

نظر به این‌که ابعاد و جنبه‌های مختلف تدوین دکترین سایبری دفاعی امنیتی ج.ا.ایران، دارای ابهامات فراوانی است لذا تبیین برخی از مبانی نظری ازجمله مبانی تدوین، منابع ورودی و سؤالات اساسی که دکترین سایبری باید به آن پاسخ بدهد از اهداف پژوهش است.

پیشینه تحقیق

با توجه به تغییرات سریع در تهدیدات سایبری و تحول پیوسته ویژگی‌های این حوزه، تدوین دکترین‌های سایبری هم در سطح بین‌المللی و هم در سطح بومی به یک ضرورت راهبردی بدل شده است. در سطح بین‌المللی، مطالعات متعددی بر لزوم انعطاف‌پذیری، تاب‌آوری و توان تطبیق با حملات سایبری تأکید دارند. به عنوان مثال، محمّد و همکاران (۲۰۲۳) بر ضرورت اتخاذ راهبردهای یکپارچه جهت محافظت از زیر ساخت‌های ملی – نمونه‌ای از کشورهایی مانند سومالی – تأکید می‌کنند که این رویکرد، تاب‌آوری را به عنوان یکی از ارکان اصلی امنیت سایبری معرفی می‌کند. در همین راستا، مطالعات Pöyhönen و Lehto (2024) لزوم ایجاد آگاهی موقعیتی مشترک و اتخاذ تصمیم‌گیری‌های غیرمتمرکز در عملیات‌های نظامی از طریق جنگ محور شبکه را برجسته می سازد؛ امری که در مواجهه با تهدیدات پیچیده، مرز بین حوزه‌های نظامی و غیرنظامی را مبهم می‌کند.

تحولات ژئوپلیتیکی نیز نقشی کلیدی در شکل‌گیری دکترین‌های سایبری ایفا می‌کند. به عنوان نمونه، جنگ رو سیه و اوکراین نمونه عینی از ادغام توانمندی‌های سایبری در راهبردهای نظامی به شمار می‌رود؛ ساریمین و دامایانتی (۲۰۲۴) راهبردهای اوکراین را در مقابله با تهدیدات سایبری روسیه بر مبنای دکترین گراسیموف – که از جنگ هیبریدی و عملیات‌های سایبری حمایت می‌کند –

تحلیل می‌کنند. افزون بر این، Veljković (۲۰۲۴) بر ضرورت تدوین راهبردهای جامع سایبری تأکید دارد که جنبه‌های تهاجمی و تدافعی را در بر بگیرد؛ در حالی که عدم وجود توافق‌نامه‌های بین‌المللی جهت تنظیم فعالیت‌های سایبری، روند تدوین دکترین‌های کارآمد را با چالش مواجه می‌سازد.

از سوی دیگر، فناوری‌های نوین به‌ویژه هوش مصنوعی، زمینه تغییر پارادایم‌های سنتی امنیت سایبری را فراهم آورده‌اند. پاپاژورگیو و همکاران (۲۰۲۴) نحوه بهره‌برداری از هوش مصنوعی در توسعه سلاح‌های پیشرفته سایبری را مورد بررسی قرار می‌دهند و این امر، لزوم بازنگری مداوم در دکترین‌های سایبری را اجتناب‌ناپذیر می‌سازد. در همین راستا، تحلیل فنسترماچر و همکاران (۲۰۲۳) پیامدهای جنگ شناختی و کاربرد ابزارهای دیجیتال در تأثیرگذاری بر دشمنان را مورد توجه قرار داده و ادغام هوش مصنوعی را به عنوان عامل تغییر در راهبردهای جنگ سایبری معرفی می‌کند. همچنین، ابعاد حقوقی و اخلاقی این حوزه از طریق پژوهشIgakuboon (۲۰۲۲) مورد بحث قرار گرفته است؛ وی به کاستی‌های حقوق بشردوستانه بین‌المللی در مواجهه با پیچیدگی‌های جنگ‌های سایبری اشاره نموده و لزوم تدوین معاهده‌ای جدید جهت حفاظت از غیرنظامیان را مطرح می‌کند.

در بستر بومی، پژوهش‌هایی به منظور تدوین الزامات دکترین سایبری در جمهوری اسلامی ایران انجام شده است. مرادی و همکاران (۱۴۰۱) در مقاله‌ای با رویکرد کیفی و استفاده از مصاحبه‌های کانونی و تحلیل مضمون، اصول و قواعد تدوین دکترین سایبری در حوزه دفاعی–امنیتی ایران را با استناد به اسناد بالادستی و دیدگاه خبرگان شناسایی و طبقه‌بندی نموده‌اند؛ نتایج این مطالعه می‌تواند راهگشای تدوین سیاست‌ها و راهبردهای مناسب در حوزه فضای سایبری باشد. به‌طور مشابه، خسروی و احمدوند (۱۴۰۰) با بهره‌گیری از روش‌های کتابخانه‌ای و تحلیل

تطبیقی، چارچوب مفهومی جهت استخراج یا بازتعریف دکترین و بررسی مولفه‌هایی نظیر راهبرد، سیاست، باور، ارزش و نگرش را ارائه نموده‌اند؛ این رویکرد می‌تواند سازمان‌ها را در تصمیم‌گیری‌های راهبردک و تطبیق با تغییرات محیطی یاری رساند.

علاوه بر این، کتاب «مقدمه‌ای بر تحلیل و هدف‌گذاری سایبری» (۲۰۲۲) نقش خط‌مشی را به عنوان ابزاری کلیدی در چارچوب‌بندی پاسخ به حملات سایبری تشریح می‌کند؛ این اثر نمونه‌هایی از نحوه استفاده از مقرراتی نظیر GDPR در اتحادیه اروپا و راهبرد سایبری وزارت دفاع (DOD)در قالب نشریات مشترک را ارائه می‌دهد و بستر قانونی و راهبردی لازم برای تدوین دکترین‌های سایبری را به نمایش می‌گذارد.

همچنین، اندیشکده امریکن اینترپرایز (۲۰۱۷) در پژوهشی با عنوان «دیدگاه‌های ایران درباره جنگ: درک دکترین‌های در حال تحول تهران»، ماهیت دکترین‌های نظامی ایران را از منظر تدافعی بررسی کرده و چهار هدف اصلی شامل امنیت ملی، دفاع سرزمینی، بازدارندگی نمایش محور و بازدارندگی تلافی‌جویانه را به عنوان مولفه‌های کلیدی معرفی می‌کند. در سال ۲۰۱۸، سارا پ وایت در مقاله «درک جنگ سایبری (درس‌های آموخته شده از جنگ روسیه-گرجستان)» تأکید دارد که موفقیت یک نیروی سایبری آموزش‌دیده مستلزم ترکیبی از دکترین، آموزش، فناوری، فرماندهی و کنترل و زیرساخت‌های فیزیکی قوی است؛ عدم وجود دکترین مشخص، توان مقابله ایالات متحده در برابر تهدیدات دیجیتال را محدود می‌کند. افزون بر این، مارتین ماتیشاک و همکاران (۲۰۱۸) با بررسی تقسیم نقش امنیت سایبری میان سازمان‌ها، خلأ موجود در تدوین دکترین‌های مشخص در حوزه جنگ سایبری را به عنوان عاملی مؤثر بر توانایی مقابله با تهدیدات دیجیتال از سوی دشمنانی نظیر روسیه و گروه‌های تروریستی مانند داعش مطرح می‌کنند.

در مجموع، ادغام نتایج پژوهش‌های بین‌المللی و بومی نشـــان می‌دهد که تدوین دکترین‌های سایبری، چه از منظر انعطاف‌پذیری و تاب‌آوری در برابر تهدیدات، چه در بســـتر تحولات ژئوپلیتیکی، بهره‌گیری از فناوری های نوین و همچنین ایجاد چارچوب‌های قانونی و اخلاقی، نیازمند رویکردی جامع و چندبعدی اســت. تلفیق این رویکردها می‌تواند زمینه‌ســاز ایجاد ســیاســت‌ها و راهبردهای مؤثری گردد که پا سخگوی چالش‌های پیچیده فضای سایبری، به ویژه در جمهوری ا سلامی ایران باشد.

مبانی نظری تحقیق

فلسفه فناوری

«مارتین هایدگر» یکی از معدود فیلسوفانی ا ست که به مسئله فناوری به‌عنوان یک مسئله فلسفی نگریسته و نگاهی عمیقاً فیلسوفانه به مو ضوعی به‌ظاهر غیر فلسفی افکنده و آن را مو ضوع تفکر عمیق فلسفی (وجودی) قرار داده ا ست. «هایدگر» با بررسی بنیادهای انتولوژیک فناوری تلاش کرد تا ما را از تفسیر و تعبیرهای ساده و پیش‌پاافتاده ابزارانگارانه و انســان مدار، نجات داده و به نقد تعابیر و تفاســیر ذهنی گرایانه از آن بپردازد...«هایدگر» می گوید: «فناوری با ماهیت فناوری معادل نیســت، وقتی که ما در جســـتجوی ماهیت «درخت» هســـتیم باید دریابیم که آنچه در هردرختی، از جهت درخت، حضور همه‌جانبه دارد، خود درختی نیست که در میان همه دیگر درختان یافت شود...به همین منوال، ماهیت فناوری هم به هیچ‌وجه امری فناورانه نیست».

از دیدگاه «هایدگر» می توان گفت که در دوره ظهور فناوری، مهم‌ترین تحولی که رخ‌داده این اســت که نگاه ما به جهان عوض‌شــده و درک تازه‌ای از آن به‌جای درک

پیشین نشسته است. ازنظر او داشتن چنین درکی از جهان شرط امکان اشتغال ما به آن فناوری‌هایی است که امروزه ابداع می‌کنیم. (علی زمانی، ۱۳۷۹)

مبانی فضای سایبر

فضا در مفاهیم جغرافیایی بخشی از طبیعت است که در رابطه با محیط‌زیست انسانی معنای جغرافیایی- انسانی می‌یابد و در برخی از منابع فارسی فضا با مکان یکسان فرض شده است. لیکن فضا در مباحث جغرافیای سیاسی شامل محیط انسانی است با همه پدیده‌های مربوط به آن. به‌عبارت‌دیگر فضا مفهومی جغرافیایی است که در فرجام کنش بازیگران انسانی و سیاسی با مکان‌های مختلف جغرافیایی و در قلمرو حیات جمعی شکل‌گرفته و از این نظر دربرگیرنده تمام عرصه‌های حیات انسانی، اعم از اقتصاد، سیاست، فرهنگ و غیره است.

فضای مجازی و فضای سایبری دو مفهوم جداگانه و مکمل هستند که فضای سایبر اسباب و وسایل رسیدن به فضای مجازی خوانده می‌شود. فضای مجازی در حقیقت تصویری از زمان و مکان فشرده شده به‌وسیله ادوات و ابزار الکترونیکی به صورت فضایی است و از حدود طبیعی مکان (کشور، مرز و سرزمین) درمی گذرد و دنیای فرضی ماورای سرزمین و مرز را در ذهن و در عمل ارتباطات و مبادلات اقتصادی بین‌المللی مطرح می‌سازد. (مجتهدزاده، ۱۳۹۱،۶۰)

رویکردهای فضای سایبری

در دو دهه اخیر، فناوری اطلاعات، ساختار جهان معاصر را دگرگون ساخته است و دامنه این تأثیرگذاری در عرصه‌های مختلف اجتماعی، اقتصادی، فرهنگی و سیاسی کاملاً محسوس است. در اینجا به سه رویکرد کلی فضای سایبری می‌پردازیم.

رویکرد لیبرالیســت ســایبری: این رویکرد که بر مبنای نظریات حاکمان فناوری تبیین شده به آزادی بی‌حدومرز در فضای سایبر می‌پردازد و دولت‌های مسلط می‌توانند هر نوع بهره‌برداری سوء را از این فضا بنمایند.

رویکرد اجتماعی- حقوقی و فنی: بر طبق نظریه لسـیگ (اسـتاد حقوق دانشـگاه هاروارد) نه‌تنها دولت، بلکه مردم و شـرکت‌ها نیز اینترنت را تنظیم می‌کنند بنابراین اینترنت به‌جای اینکه تحت سلطه قوانین و فرمان‌ها درآمده با شد، عمدتاً به‌و سیله معماری یا کد، سخت‌افزار و نرم‌افزار که همگی باهم فضای مجازی را شکل می دهند، تنظیم می‌شود. (جمشیدی بروجردی،۱۳۹۷،۱۰۵)

رویکرد سایبر پاترنالیستی: در این دیدگاه دولت‌ها و سازمان‌های جهانی قابلیت تنظیم مقررات در اینترنت و محدوده سرزمینی رادارند. (حسینی محمدرضا،۱۳۹۸)

سطوح جنگ سایبری

در منابع و مبانی دفاعی دنیا سطوح جنگ سنتی، سه سطح راهبردی، عملیاتی و تاکتیکی تفکیک می‌شـود. ناتو در سـال ۲۰۱۲ در کتابچه راهنمای چارچوب امنیت سایبری ملی برای تجزیه‌وتحلیل جنگ‌های سایبری چهار سطح را تعریف می‌نماید و علاوه بر سـه سـطح ذکرشـده در جنگ سـنتی، سـطح چهارمی با عنوان سـطح خط‌مشـی‌گذاری برای تعاریف اهداف بلندمدت سـیاسـت‌گذاری تعریف می‌نماید (ناتو، ۲۰۱۲: ۱۱۲-۱۰۸)

مبانی دکترین

از درون گفتمان عام، فرضـیه به وجود می‌آید و فرضـیه منتج می‌شـود به تئوری یا نظریه عام. از دل نظریه عام مفهومی به وجود می‌آید به نام پارادایم خاص، مدل خاص و گفتمان خاص. در گفتمان خاص است که نگاه‌ها و زاویه‌های دید افراد و

مکاتب م شخص می شود که خروجی آن به شرح ذیل ا ست. قلب این پنج مورد دکترین اســت و هر چه از ســمت راســت به چپ حرکت کنیم انعطاف -پذیری اندیشه کاهش می‌یابد. (سید رحمانی، ۱۳۹۳)

جدول ۱) سیر تطور گفتمان خاص

یونانی	دکسا	ایدیا	داکترینا	تنت	دگما
عربی	ظن	–	قاعده، یقین	جزم	تحجر
ایرانی	گمان	–	آموزه، آئین	–	سنگ شدن باور

دکترین پلی میان تجربیات موفق گذ شته و انتظارات آینده ایجاد می‌کند. برای تبیین در ست میان دکترین، سیا ست و راهبرد در گام اول لازم ا ست به درکی م ستقل از مفهوم امنیت د ست‌یابیم. معهذا رابطه‌ای سل سله مراتبی میان دکترین، سیا ست و راهبرد برقرار اســت. دکترین به دلیل این‌که ماهیت هدف‌گذاری دارد در رأس قرارمی گیرد. پس‌ازآن سیاست است که بیانگر هدایت امکانات موجود در راستای هدف اســت و از جنس چیســتی اســت و درنهایت راهبرد قرار دارد که چگونگی به‌کارگیری امکانات موجود برای تحقق اهداف را موردمطالعه قرار می‌دهد (خلیلی، رضا،۱۳۸۶، ۴۴۵).

سه موضوع دکترین قالب وجود دارد. اولین مورد، دکترین سیاسی است که بیشتر در قانون اســاســی یک ملت یا معادل آن منعکس می‌شــود. مورد دوم دکترین‌های حقوقی است که اغلب دکترین‌های سیاسی را به‌عنوان تجسم تعامل اجتماعی دنبال می‌کنند. آخرین مورد دکترین نظامی اســت که بر چگونگی حکمرانی یک ملت در تلاش برای تأمین امنیت خود دلالت دارد. دکترین نظامی را می‌توان به دکترین‌های پایه، محیطی و سازمانی تقسیم کرد (جانشسکی و کلاریک،۲۰۱۲) دکترین نظامی

دارای سطوح راهبردی، عملیاتی و تاکتیکی است (ثروتی،۱۳۸۹:۲۷). انواع دکترین‌ها به‌اختصار در جدول ۲ بیان گردیده است.

جدول ۲) انواع دکترین (نوذری،۱۳۹۸ جلسات تدوین دکترین)

سطوح دکترین	انواع دکترین					
ملی	ملی	دفاعی- امنیتی	نظامی	سیاسی	اقتصادی	فرهنگی
کلان ن.م.	نظامی	نظامی- امنیتی		امنیتی		نظامی
نیرویی	هوایی	زمینی	دریایی	فضایی	عملیات مشترک	عملیات مرکب
رویکردی	تهاجمی	تدافعی	دفاع پیشگیرانه			دفاع بازدارنده

مبانی تدوین دکترین

تدوین دکترین، مستلزم شناخت عمیق از وضع موجود و آینده مطلوب است. اصول بنیادین و قواعد پایه دکترین ریشه در ارزش‌ها و هنجارهای ملی دارد. به‌عنوان‌مثال، از دیدگاه خلیلی، تدوین دکترین امنیت ملی، در قالب مثلثی از اهداف و آرمان‌های ملی، ارزش‌ها و هنجارهای ملی و منافع و مصالح ملی امکان‌پذیر است که اهداف و آرمان‌های ملی در رأس این مثلث قرار دارند معهذا دکترین امنیت ملی حاصل جمع و برآیند هر سه عنصر است که در کنار یکدیگر ترسیم‌کننده وضعیت مطلوب برای هر کشور هستند (خلیلی، ۱۳۸۶:۴۴۱).

هنگامی که تغییراتی در محیط و عوامل مؤثر در دکترین رخ می‌دهد، تجارب تازه‌ای حاصل می‌شود و یا این‌که نظریه‌ای جدید ابراز می‌شود، فرایند توسعه دکترین جاری یا تدوین دکترین جدید آغاز می‌شود. این مراحل عبارت‌اند از:

جمع‌آوری اطلاعات، تدوین و توسعه دکترین و انتشار آن (دانش آشتیانی، ۱۳۸۸: ۵۶).

ازنظر دکتر نوذری خاستگاه دکترین را در چهار منظر می‌توان جستجو نمود که عبارت‌اند از تاریخ، تجربه، تئوری، تمرین و ممارست (جلسات تدوین دکترین، ۱۳۹۸). به‌عبارت‌دیگر مجموعه تجربیاتی که در طول سالیان بعضاً طولانی اندوخته می شود و از طریق تمرین و تکرار در بوته آزمایش قرار می‌گیرد قابلیت تبدیل‌شدن به یک عبارت دکترینی را خواهد داشت. البته این امر در مباحث نظامی به‌صورت بارزتری ملموس است.

منابع ورودی تدوین دکترین

برر سی دکترین‌های منت شر شده در دنیا این نکته را به ذهن متبادر می‌کند که این اسناد دارای بخش‌های طبقه‌بندی‌شده‌ای می‌باشند که منتشر نمی‌گردند و بخش‌های در د سترس غالباً جنبه بازدارندگی دارند و هیچ‌گونه چارچوب خا صی جهت تدوین دکترین از مرجع ر سمی ارائه نگردیده ا ست. معهذا برخی ازنظرات در خصوص منابع ورودی تدوین دکترین ارائه می‌شود:

جدول ۳) منابع ورودی تدوین دکترین

مؤلف	منابع ورودی تدوین دکترین
باقری افشردی	مأموریت‌های نیرو؛ تجارب دفاع مقدس، تجارب جنگ‌های اخیر آمریکا؛ توانایی‌های نیروها؛ ساختار نیروها؛ فناوری موجود؛ نتایج رزمایش‌ها، آموزش‌ها، تمرین‌ها و تجارب؛ سازمان‌دهی در نیروها؛ ساختار و تجهیزات نیروها؛ آموزش ـ نحوه عمل ـ رزمایش و تمرین؛ جغرافیای کشور (طبیعی و انسانی)؛ مجموعه‌ای از توان عملیاتی، پشتیبانی، سایر ابعاد؛ تهدید و سناریوهای آن، دکترین عملیاتی دشمن؛ روابط با همسایگان. (۱۳۹۶: ۱۰-۱۱)

آقا محمدی	قرآن کریم و روایات (به‌ویژه نهج‌البلاغه)؛ اندیشه‌های نظامی رهبری نظام؛ مأموریت‌ها و وظائف نیروهای مسلح؛ مطالعه محیط؛ تجارب نظامی، فن‌آوری‌های نظامی (۱۳۸۹)
نوذری	فرامین، تدابیر و رهنمودهای ابلاغی، اندیشه و ایدئولوژی حاکم بر ارزش‌های سازمانی، قوانین و مقررات، دکترین ملی کشور، راهبرد فرا سازمانی، اهداف سازمانی، محیط بین‌المللی، روابط میان سازمان‌های مختلف محیط داخلی، تجارب سازمانی، ملاحظه‌های ژئوپلیتیکی کشور، توسعه فن‌آوری و الزام‌ها و مقدورات سازمانی، وسایل و تجهیزات (۱۳۸۹)
ثروتی	فرامین، تدابیر و رهنمودهای ابلاغی، قوانین و مقررات، سیاست‌های دفاعی امنیتی در سطوح مختلف، تصور جنگ آینده (سناریوها)، توسعه فناوری، مقدورات نظامی، تجربه‌های دفاع مقدس و سایر تجربه های سازمانی، مدل عملکرد دشمن (۱۳۸۹،۴۶-۴۷)
ن.م آمریکا	قوانین اساسی، سیاست‌های دفاعی و امنیتی، راهبردی، نظریه، فناوری، تجربه (ثروتی،۱۳۹۱: ۱۵۴)
دفاع ملی انگلیس	منافع ملی، اهداف نظامی ملی، دشمن فرضی، سیاست و خط‌مشی، نظریه، تاریخچه (ثروتی،۱۳۹۱: ۱۵۴)

پرسش‌های کلیدی دکترین سایبری دفاعی امنیتی

تدوین دکترین درواقع پاسخ به سه سؤال کلیدی چیستی، چرایی و چگونگی است که پاسخ این سؤالات پاسخگوی بخش‌های مختلف فضای سایبر هستند. مقاله ایجاد دکترین جنگ سایبری جانشسکی و کلاریک پرسش‌های راهبردی ذیل را به‌عنوان نمونه‌های مهمی از سؤالات موردنیاز برای تدوین یک دکترین سایبری ارائه می‌دهد.

۱- خطوط حدفاصل بین جنگ سایبری و جنگ سنتی چیست؟

۲- فضای درگیری در دکترین جنگ سایبری کجاست؟

۳- دکترین جنگ سایبری چه آستانه تحملی را برای انجام واکنش را مجاز می‌داند؟

۴- دکترین جنگ سایبری چه تعریفی از پیروزی دارد؟

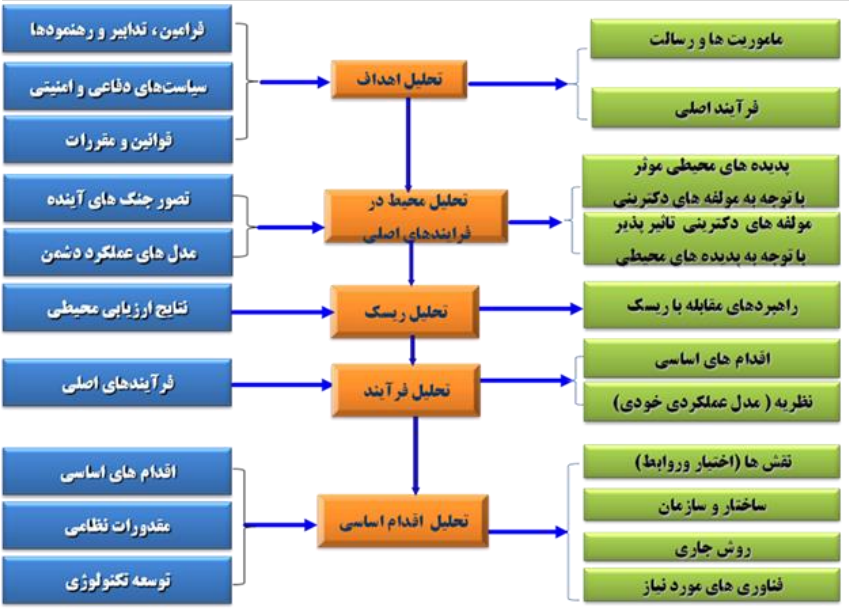
۵- سرمایه‌های اصلی دکترین جنگ سایبری برای پیروزی چیست؟

۶- عوامل مؤثر بازدارندگی و پاسخگویی دکترین جنگ سایبری چیست؟

مدل‌های تدوین دکترین

طبق بررسی‌های به‌عمل‌آمده تاکنون جهت تدوین دکترین سایبری در ج.ا.ایران روش تدوین‌شده‌ای وجود ندارد؛ لیکن چند نمونه از روش‌های متداول تدوین دکترین که قابلیت بهره‌برداری به‌عنوان مبنایی جهت تدوین دکترین سایبری را دارند، به شرح ذیل بررسی می‌گردد:

مدل سیستمی: این مدل توسط هیأت عالی آئین‌نامه‌های ن.م ارائه شده است. در این مدل، خلق یا تجدیدنظر در یک دکترین جدید در طی پنج مرحله به شرح ذیل انجام می‌پذیرد. از ویژگی‌های منحصربه‌فرد این مدل آن است که باعث می‌گردد تا فعالیت‌های انجام‌شده در گروه‌های تدوین‌کننده دکترین از چارچوب واحدی پیروی کرده و ضمن ایجاد یکنواختی، امکان ارزیابی را برای اطمینان از توجه همه‌جانبه به اجزای دکترین فراهم نماید.



شکل ۱) فرآیند پنج مرحله‌ای تدوین دکترین (ثروتی، ۱۳۹۱: ۱۸۳)

مدل دکترین نظامی: دکتر دانش آشتیانی در مقاله‌ای با عنوان "اصول و روش تدوین دکترین نظامی" با بهره‌مندی از چند منبع خارجی، ضمن تبیین ماهیت دکترین با اشاره به اصول جنگ و رابطه آن با 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) (دانش آشتیانی، ۱۳۸۸: ۶۰)

مدل تدوین دکترین در روسیه: عبدالرسول دیو سالار در مقاله خود به تشریح روش تدوین دکترین در رو سیه می‌پردازد. و بیان می‌کند که مفهوم دکترین در ادبیات شرق و غرب از تفاوت قابل‌توجهی برخوردار است. در ادبیات شرقی دکترین نقش محوری در انتقال دیدگاه‌ها و باورهای رسمی نسبت به جنگ آینده و محیط امنیتی

پیش رو دارد. در حالی که در غرب دکترین شـــعور ناپیدای حاکم بر به کارگیری نیروهای مسلح در صحنه نبرد تعبیر می شود که بر پایه مفاهیم عملیاتی شکل‌گرفته و ارتباط میان فناوری، ســـاختار، تئوری و تجربه رزمی را برقرار می‌ســـازد در شـــرق دکترین برداشـــت مشـــترکی اســـت از مطالبات دفاعی ملی. (دیوســـالار، عبدالرسول،۱۶:۱۳۸۶)

شکل ۲) مدل تدوین دکترین در روسیه

روش‌شناسی تحقیق

این تحقیق برمبنای نتایج از نوع کاربردی است زیرا نتایج حاصله در عمل می‌تواند مبنای تدوین‌کنندگان دکترین ســایبری قرار گیرد. تحقیق حاضــر برمبنای اهداف از نوع توصیفی- تحلیل و برمبنای داده‌ها از نوع کیفی است. جامعه آماری آن مشتمل بر منابع علمی داخلی و خارجی جامعهٔ آماری این تحقیق شـامل اسـناد منابع علمی معتبر داخلی و خارجی در حوزه دکترین، سایبر و دفاع و امنیت است که از شیوی نمونه‌گیری هدفمند استفاده شده است. روش گردآوری داده‌ها به روش کتابخانه‌ای به‌وسیله پیمایش اسناد با ابزار فیش‌برداری است.

پایایی اسناد و مدارک

ازآنجایی‌که این تحقیق از نوع کیفی ا ست لذا محقق برای پایایی تحقیق کیفی اقدام به مســـتند نمودن اســـناد و مدارک موجود جهت تعیین الزامات موردنیاز تدوین دکترین سایبری ج.ا.ایران اقدام نموده است.

روایی بررسی اسناد و مدارک

ازآنجایی‌که این تحقیق از نوع تو صیفی ا ست لذا ضروری ا ست که روایی تحقیق ازنظر ســـاختاری موردبررســـی قرار گیرد. برای بالا بردن روایی تحقیق ازنظر ســـاختاری، محقق اقدام به جمع‌آوری داده‌ها از چندین منبع مختلف و تطبیق و مقارنه آن‌ها پرداخته اســـت که برای نمونه به مقاله ایجاد دکترین جنگ ســـایبری و همچنین پژوهش‌های منابع معتبر داخلی و پژوهشـــکده امریکن اینترپرایز اشـــاره نمود.

تحلیل داده‌ها و نتیجه‌گیری

ما در این مقاله ضمن بر شمردن فضای جدید متأثر از فضای سایبر و تأثیری که این فضا بر امنیت ملی ج.ا.ایران خواهد گذا شت و همچنین اهمیت و ضرورت تدوین دکترین ســـایبری حوزه دفاعی و امنیتی، نیازمندی کشـــور را به این ســـند بالادستی مهم تبیین نمودیم. از سوی دیگر لزوم ابداع یک الگوی تدوین دکترین سایبری منطبق با بافتار و ساختار جمهوری اسلامی ایران کاملاً محسوس است. لیکن این مدل با توجه به مدل های پیشـــین دکترین بومی و همچنین اعمال ویژگی‌های فضای سایبر به نظر قابل‌دسترسی است.

از دیدگاه «هایدگر» در دوره ظهور فناوری، مهم‌ترین تحولی که رخ‌داده این اســـت که نگاه ما به جهان عوض‌شـــده، انســـان «فناوری» را برای رســـیدن به اهدافش به

وجود آورده ا ست. ماهیت فناوری هم به‌هیچ‌وجه امری فناورانه نی ست«هایدگر» با این بیان و تمثیل می‌خواهد ما را از سطحی‌نگری نسبت به ماهیت فناوری نجات داده و ذهن ما را به آن امری که چون یک روح در همه جلوه‌های فناوری حضور دارد، معطوف نماید.

ف ضای مجازی و ف ضای سایبری دو مفهوم جداگانه و مکمل ه ستند که ا سباب و وسایل رسیدن به فضای مجازی، فضای سایبری خوانده می‌شود. فضای مجازی در حقیقت ت صویری از زمان و مکان ف شرده شده به‌و سیله ادوات و ابزار الکترونیکی به صورت ف ضایی ا ست و از حدود طبیعی مکان (ک شور، مرز و سرزمین) درمی گذرد و دنیای فرضی ماورای سرزمین و مرز را در ذهن و در عمل ارتباطات و مبادلات اقتصادی بین‌المللی مطرح می‌سازد.

رویکرد خالقان و تابعان فناوری به آن به شدت متفاوت ا ست که این امر موجب به وجود آمدن رویکردهای متفاوت در حوزه سایبری شده ا ست که به سه رویکرد قالب در مقاله توجه شده ا ست که این رویکردها از گمنامی و آزادی بی وحد مرز در ف ضای مجازی آغاز و به و ضع تنظیم مقررات در اینترنت و محدوده سرزمینی می‌انجامد.

دکترین دربرگیرنده سه مؤلفه ا سا سی چی ستی، چرایی و چگونگی ا ست و دارای ماهیتی نظری و نرم است و موجب تحکیم حاکمیت و اقتدار ملی و تقویت بنیه دفاعی- امنیتی کشور می‌گردد. تدوین دکترین که غالباً به امور نظامی برمی‌گردد بر طبق دسته‌بندی‌های مختلف دارای گروه‌بندی‌های متفاوتی است معهذا دکترین یکی از ا سناد بالاد ستی حائز اهمیت در ف ضای سایبر ا ست. دکترین در اندی شه نظامی شرق و غرب از اهمیت ویژه‌ای برخوردار است اگرچه دکترین روسی و چینی حاکی از غلبه نگاهی کل گرا و دکترین غربی نگاهی جزء گرا است که بالطبع

روش‌های تدوین آن متفاوت است. از سوی دیگر اکثر کشورها به روش تدوین آن اشاره واضحی نمی‌نمایند.

از بررسی انجام‌شده در منابع علمی داخلی و خارجی می‌توان دریافت که ورودی‌های موردنیاز در روش‌های مختلف متفاوت است هرچند اشتراکاتی هم دراین‌بین وجود دارد عوامل مذهبی، فناوری‌های موجود، تجارب نظامی از نقاط اشتراک غالب روش‌های است.

بررسی‌های به‌عمل‌آمده در خصوص روش‌های تدوین دکترین دارای اشتراکاتی است: تدوین دکترین باید در قالب چند مرحله (عمدتاً مستقل) انجام شود منابع ورودی باید در شرایط محیطی و سایر عوامل مؤثر تأثیر داده شوند، پس از تدوین دکترین فرآیند توسعه در قالب انجام بازخورد و وارد نمودن تغییرات جدید انجام می‌پذیرد. نکته حائز اهمیت در اغلب این روش‌ها عدم صراحت در استفاده از اسناد بالادستی است که به نظر می‌رسد استفاده از اسناد بالادستی به‌صورت پیش فرض در تمام روش‌ها وجود دارد.

با توجه به ثابت بودن ماهیت دکترین‌ها می‌توان از برخی از وجوه مشترک تدوین دکترین‌ها ازجمله مدل تدوین دکترین سیستمی، مدل تدوین دکترین نظامی و مدل تدوین دکترین در روسیه بهره برد لیکن در مدل‌های فوق باید ویژگی و ماهیت فضای سایبری را هم لحاظ نمود. البته در مدل تدوین دکترین سایبری باید مقتضیات و الزامات ج.ا.ایران را درج نمود.

پیشینه تحقیق (مقالات) بیانگر این موضوع است که موضوع دکترین و به‌صورت خاص دکترین سایبری دارای ادبیات مطلقاً مشترکی در کشورهای مختلف نیست و حتی برای دکترین در حوزه خاص نیز تعاریف گوناگونی وجود دارد و بعضاً روش‌های متعددی نیز پیشنهادشده است. علاوه بر پیشینه درج‌شده در مقاله محقق

مقالات و روش‌های دیگری را نیز مطالعه کرده است ازجمله مدل لونی، نیروی هوایی انگلیس، ارتش آمریکا و... که این امر اثباتی بر تکثر در روش‌های دکترین است. لیکن آنچه بررسی عمیق پیشینه‌ها نشان می‌دهد بیانگر اذعان اغلب کارشناسان حوزه امینت ملی و دفاع و امنیت به نقش وحدت‌آفرین و ضرورت تدوین دکترین در سطوح مختلف است و در جهت افزایش اثربخشی دکترین‌های مدون نوشته شده، تدوین دکترین در همه حوزه‌ها موجب تکمیل نقشه راه امنیت ملی می‌گردد که هر یک از دکترین‌ها فقط بخشی از دکترین امنیت ملی را پوشش می‌دهد. یافته‌های محقق بر مبنای اسناد موجود مبین این امر است که دکترین نسبت به سیاست و راهبرد در جایگاه بالاتری قرار دارد چون ماهیت هدف‌گذاری دارد و از جنس کجایی است. پس‌ازآن سیاست و درنهایت راهبرد قرار دارد. به‌علاوه دکترین سایبر، بازدارندگی سایبر را به میزان قابل‌توجهی امکان‌پذیر می‌کند. بازدارندگی بر اساس فرضیات اساسی مبنی بر اینکه چه کسی و چگونه می‌تواند برحذرشود.

در تنها مدل ارائه شده دکترین جنگ سایبری، به آغاز صدور این فرآیند از سوی بالاترین مقام حکومتی و همچنین در آخرین مرحله تصویب و ابلاغ آن از سوی ایشان است. در این مدل به شدت سعی شده است که توجه ویژه‌ای به بازیگران عرصه سایبری (دولت، سازمان‌های بزرگ و بخش خصوصی) و همچنین اعمال‌نظر کلیه بازیگران و کسب نظر موافق آن‌ها در تدوین دکترین سایبری شده است.

پیشنهادها

با توجه به ویژگی‌های خاص فضای سایبر که علاوه بر ویژگی‌های به ارث برده از فضای حقیقی از پویایی بالایی برخوردار است لذا جهت تدوین دکترین در این فضا در حوزه دفاعی امنیتی نیازمند یک روش منحصربه‌فرد است هرچند تدوین

روش آن با مشترکاتی با سایر دکترین‌ها نیز دارد معهذا پیشنهادی می‌گردد روش تدوین دکترین سایبری در حوزه دفاعی امنیتی ج.ا.ایران احصاء و پس از اعتبارسنجی به بازیگران ذی مدخل ارائه گردد.

از سوی دیگر تدوین هر دکترین نیازمند یک نظریه دکترینی یا هسته دکترینی است که تمامی اصول تدوین شده حول هسته اصلی دکترین صورت می‌پذیرد. سؤال اساسی که در جهت تدوین دکترین سایبری دفاعی امنیتی ج.ا.ا مطرح است احصاء هسته دکترینی یا نقطه کانونی این دکترین است که نیازمند پژوهش مستقل و جداگانه‌ای است.

پاسخ به سؤالات مطروحه در مقاله جهت تدوین دکترین ازجمله تعیین خطوط حدفاصل فی‌مابین جنگ سنتی و جنگ سایبری، تعریف آستانه تحمل یک کشور در پاسخگویی به حملات سایبری، تعریف پیروزی و جنگ سایبری ازجمله سؤالات اساسی است که در راستای تدوین دکترین سایبری در قالب یک موضوع تحقیقاتی قابل‌بررسی است.

نوآوری تحقیق

۱- تعریف یک سطح جدید از جنگ سایبری: در این مقاله پیشنهاد می‌شود که جنگ سایبری به‌عنوان یک سطح مستقل در کنار سطوح جنگ سنتی تعریف شود. این موضوع در تحلیل‌های راهبردی جدید است و می‌تواند چارچوب جدیدی برای سیاست‌گذاری دفاعی ایجاد کند.

۲- ایجاد مدل بومی تدوین دکترین سایبری: در این مقاله سعی شده یک مدل بومی برای تدوین دکترین سایبری جمهوری اسلامی ایران پیشنهاد شود که متناسب با مقتضیات امنیت ملی کشور باشد.

۳- پرداختن به اهمیت دکترین در اسناد بالادستی: مقاله به اسناد بالادستی جمهوری اسلامی ایران در حوزه فضای سایبری پرداخته و جایگاه دکترین سایبری را در نظام امنیتی کشور تبیین کرده است.

۴- تحلیل تأثیرات فضای سایبری بر امنیت ملی: مقاله تلاش دارد تا نشان دهد که فضای سایبری یک بخش اساسی از امنیت ملی است و کشورها نیازمند رویکردهای راهبردی برای مقابله با تهدیدات این حوزه هستند.

منابع

الف- منابع فارسی

۱. مجموعه بیانات امام خامنه‌ای (مدظله‌العالی) قابل‌دسترسی در: www.khamenei.ir

۲. آقا محمدی، داود (۱۳۸۹) جلسه تدوین دکترین نظامی ستاد کل نیروهای مسلح، تهران.

۳. افشردی، محمدحسین؛ عراقی، عبدالله؛ زین‌الدینی، مجید (۱۳۹۶) اصول دکترین عملیاتی نزاجا و نزسا درنبرد ناهمطراز، فصلنامه مطالعات دفاعی راهبردک، سال پانزدهم، شماره ۷۰، صص: ۵-۳۲.

۴. ثروتی، محسن و همکار (۱۳۸۹) راهنمای تدوین دکترین در حوزه نظامی، ناشر دبیرخانه هیأت عالی تجدید نظر در آئین نامه های نیروهای مسلح ستاد کل نیروهای مسلح، تهران .

۵. دانش آشتیانی، محمدباقر. (۱۳۸۸). اصول و روش تدوین دکترین نظامی. فصلنامه نظم و امنیت انتظامی، شماره سوم سال دوم. صص: ۱۷-۷۱.

۶. سند راهبردی جمهوری اسلامی ایران در فضای مجازی (مصوب سال ۱۴۰۱).

۷. ثروتی، محسن و همکاران (۱۳۹۱) راهنمای آموزشی تدوین دکترین، تهران، انتشارات دبیرخانه هیئت عالی آئین نامه های نیروهای مسلح.

۸. جمشیدی بروجردی، علی رضا و همکار (۱۳۹۷) طراحی چهارچوب مفهومی خط‌مشی های تنظیمی در حوزه محتوای فضای مجازی جمهوری اسلامی ایران ، فصلنامه علمی - پژوهشی سیاستگذاری عمومی دروه ۴، شماره ۱، بهار ۱۳۹۷.

۹. حکم تشکیل و انتصاب اعضای شورای عالی فضای مجازی توسط امام خامنه‌ای (مدظله‌العالی) در سال ۱۳۹۰

۱۰. حکم انتصاب اعضای شورای عالی فضای مجازی توسط امام خامنه‌ای (مدظله‌العالی) در سال ۱۳۹۴

۱۱. حسینی ،محمدرضا؛ (۱۳۹۸)جزوه درسی حقوق و قوانین سایبری، دانشگاه عالی دفاع ملّی، تهران.

۱۲. خسروی، عباس، و احمدوند، علی محمد. (۱۴۰۰). الگوی تعیین دکترین در طرح ریزی و برنامه‌ریزی راهبردی. مطالعات راهبردی ناجا، ۶(۲۱)، ۲۳-۴۵.

۱۳. خلیلی، رضا. (۱۳۸۶). دکترین، سیاست و راهبرد؛ نسبت سنجی نظری و مفهومی. فصلنامه مطالعات راهبردی، سال دهم شماره ۳، صص: ۴۲۳- ۴۵۰.

۱۴. دیوسالار،عبدالرسول (۱۳۸۶) ، ارزیابی ابعاد گوناگون دکترین‌های امنیتی- دفاعی روسیه، مجله سیاست دفاعی، سال پانزدهم، شماره پیاپی ۶۰، پاییز ۱۳۸۶.

۱۵. سید رحمانی (۱۳۹۳) مفهوم واژه دکترین، سایت اندیشکده یقیین.

۱۶. علی زمانی، امیرعباس (پاییز ۱۳۷۹)، ماهیت تکنولوژی از دیدگاه هایدگر، مجله: نامه مفید، صفحات: ۱۹۷-۲۲۲.

۱۷. عمید، حسن (۱۳۸۴). فرهنگ فارسی: انتشارات امیرکبیر. تهران .

۱۸. مجتهدزاده، پیروز (۱۳۹۱) ، ژئوپولیتیک فضای مجازی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات.

۱۹. مرادی محمدرضا ، ولوی محمد رضا، حسینی محمدرضا و نوروزانی شهرام (۱۴۰۱)، اصول وقواعد دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی- امنیتی، فصلنامه راهبرد دفاعی، دوره ۲۰ شماره ۷۹، صص:۴۴-۷۳.

۲۰. معمارزاده، غلامرضا. پورشاسب، عبدالعلی. (۱۳۸۶). الگوی مفهومی دکترین نظامی. فصلنامه مطالعات دفاعی راهبردک. سال هشتم شماره ۳۰ صص: ۱۸۷-۲۱۲.

۲۱. نوذری فضل‌الله، (۱۳۸۹)، جزوه آموزشی دکترین رزم زمینی در محیط جنگ ناهمگون، دانشگاه امام حسین علیه‌السلام سپاه پاسداران انقلاب اسلامی.

۲۲. نوذری فضل الله (۱۳۹۸) جلسات آموزشی تدوین دکترین، تهران.

ب- منابع انگلیسی

23. KevinRoberts(2023) Mandate for Leadership : The Conservative Promise (PROJECT2025) , Heritage Foundation's.
24. Couretas, J.M. (2022). Cyber Policy, Doctrine, and Tactics, Techniques, and Procedures (TTPs). In: An Introduction to Cyber Analysis and Targeting. Springer, Cham.
25. Mohamed, M., Jasim, O., Sameer, A., Ali, H., & Hajon, Y. (2023). Integrated cyber resilience strategy for safeguarding the national infrastructure of somalia: addressing threats. World Journal of Advanced Research and Reviews, 20(2), 1291-1299.

26. Pöyhönen, J. and Lehto, M. (2024). Architecture framework for cyber security management. European Conference on Cyber Warfare and Security, 23(1), 388-397.

27. Sarimin, B. and Damayanti, A. (2024). Ukraine's strategy to counter russian cyber threats in the russo–ukrainian war. International Journal of Social Science and Human Research, 07(11).

28. Veljković, S. (2024). Possibility of applying the rules of international humanitarian law to cyber warfare. Pravo - Teorija I Praksa, 41(3), 17-28.

29. Fenstermacher, L., Uzcha, D., Larson, K., Vitiello, C., & Shellman, S. (2023). New perspectives on cognitive warfare.

30. Igakuboon, A. (2022). An appraisal of the legal framework for the protection of civilians in cyber-warfare under international humanitarian law. International Journal of Research and Scientific Innovation, 09(07), 14-26.

31. Papageorgiou, M., Can, M., & Vieira, A. (2024). China as a threat and balancing behavior in the realm of emerging technologies. Chinese Political Science Review, 9(4), 441-482.

32. Matishak, Martin ,(2018), Where's the U.S. doctrine on cyber warfare? Available at: https://www.politico.com/newsletters/morning-cybersecurity.

33. White,Sarah P. (2018) , Understanding Cyberwarfare, Lessons from the Russia-Georgia War , modern war institute at west point.

34. USA joint force development,(2018), Cyberspaces operations joint publications 3-12.

35. Jackson ,Aaron P. (2017), The Nature of Military Doctrine: A Decade of Study in 1500 Words, Available at: https://www.realcleardefense.com/articles

36. United States Department of Defense, April 2015, The Department of Defense Cyber Strategy, p. 9.

37. Mclnnis, J .Mattehw(2017) , Iranian concepts of warfare , understanding Tehran's evolving military doctrin's ,AIE ,Available at: http://www.aei.org/wp-content/uploads.

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

39. NATO CCD COE Publication (2012), National Cyber Security Framework Manual , . Available at: www.ccdcoe.org