فصلنامهٔ علمی راهبرد دفاعی، سال بیستم، شمارهٔ ۷۹، پاییز ۱۴۰۱

فرمانده معظم کل قوا: فضای مجازی بدون اختیار ما، دارد مدیریت می‌شود و عوامل مسلط بین‌المللی در این فضا به‌شدت فعال‌اند. نمی‌شود مردم‌مان را در این فضا، بی‌پناه رها کنیم. (بیانات مقام معظم رهبری (مدظله‌العالی) ۱۳۹۹/۰۶/۰۲)

مقالهٔ پژوهشی: اصول وقواعد دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی– امنیتی

20.1001.1.17351723.1401.20.79.2.2

محمدرضا مرادی[۱]، محمدرضا ولوی[۲]، محمدرضا حسینی[۳]، شهرام نوروزانی[۴]

تاریخ دریافت: ۱۴۰۱/۰۴/۰۲ تاریخ پذیرش: ۱۴۰۱/۰۶/۱۲

چکیده

بررسی حوادث دفاعی– امنیتی مبین این امر است که امنیت ملّی در جمهوری اسلامی ایران به‌شدت تحت تأثیر فضای سایبر قرارگرفته است. از سوی دیگر نظام مدیریت راهبردی دفاعی امنیتی تلاش می‌نماید، دستیابی به اهداف و نیل به خروجی‌های مورد انتظار حوزه دفاعی– امنیتی را تضمین نماید. بخش مهمی از این نظام تبیین یا تعیین مواردی مانند اصول و قواعد دکترینی، سیاست‌ها و راهبردها است. تدوین اصول و قواعد دکترین سایبری دفاعی–امنیتی موجب انسجام در رویه‌ها، ایجاد بازدارندگی مقتدرانه و کمک به جلوگیری از درگیری‌های آینده می‌شود. این مقاله در نظر دارد مبتنی بر مبانی نظری تدوین دکترین سایبری اصول و قواعد دکترین سایبری جمهوری اسلامی ایران را در حوزه دفاعی امنیتی مدون نماید.

رویکرد این تحقیق کیفی بوده و از روش گردآوری کتابخانه‌ای و میدانی (مصاحبه کانونی و مراجعه به آراء خبرگان به روش نمونه‌گیری هدفمند گلوله برفی) استفاده نموده است. محققین با بهره‌مندی از اسناد بالادستی در جمهوری اسلامی ازجمله قانون اساسی، بیانات مقام معظم رهبری (مدظله العالی) سیاست‌های کلی نظام و سایر اسناد سازمانی و حکومتی به روش تحلیل مضامین نسبت به تدوین اصول (۳ اصل) و قواعد (۱۷ مورد) دکترین سایبری در حوزه دفاعی امنیتی اقدام نموده‌اند. پایایی مفاهیم بدست آمده مبتنی بر اسناد بالادستی متقن جمهوری اسلامی بناشده است و روایی آن مبتنی بر دیدگاه کرسول و از طریق شخص ثالث بوده است.

واژگان کلیدی: دکترین، فضای سایبر، دفاعی– امنیتی.

مقدمه

۱. دکترای مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول)، این مقاله منتج از رساله دکتری است. mr.moradi@sndu.ac.ir

۲. دانشیار دانشگاه صنعتی مالک اشتر valavi@mut.ac.ir

۳. دانشیار دانشگاه عالی دفاع ملی

۴. استادیار دانشگاه عالی دفاع ملی

امروزه فضای سایبری پدیده‌ای است که نمی‌توان از آن اجتناب نمود لیکن با توجه به نبود سازوکار جدی این فضا در داخل کشور، باید بخش‌های تهدیدآمیز این فضا را بامطالعه هوشمند به فرصت تبدیل و به‌عنوان ابزاری جهت ارتقاء امنیت ملّی کشور استفاده نمود.

مطابق سند چشم‌انداز ۱۴۰۴ هجری شمسی، جامعه ایرانی امن، مستقل و مقتدراست. لیکن تهدیدات پیش روی جمهوری اسلامی ایران با اضافه شدن عرصه سایبری به عرصه‌های جنگی، به‌صورت تصاعدی افزایش‌یافته است. به‌عبارت‌دیگر امنیت ملّی ج.ا.ایران و به‌صورت خاص بخش دفاع، حوزه‌هایی هستند که به‌شدت متأثر از فضای سایبر گردیده‌اند. همچنین در برنامه راهبردی فضای مجازی جمهوری اسلامی ایران، فضای مجازی، فضایی در امتداد فضای واقعی، سالم و ایمن است.

مجموعه عوامل یادشده بالا، بازیگران فضای سایبری ج.ا.ایران در حوزه دفاعی امنیتی را به‌سوی مدیریت راهبردی (دفاعی- امنیتی) این فضا و گنجاندن توانمندی سایبری در قابلیت‌های نظامی رهنمون می‌سازد. هرچند مدیریت اعمال‌شده بر این فضا دارای نقصان‌هایی در انسجام مدیریت است تا جایی که مقام معظم رهبری(مدظله‌العالی)، می‌فرمایند «همه کشورهای دنیا، بر فضای مجازی اِعمال مدیریت می‌کنند اما در کشور ما، برخی به رها بودن فضای مجازی افتخار می‌کنند درحالی‌که این شیوه به‌هیچ‌وجه افتخار ندارد».(بیانات دوم فروردین ۱۴۰۰)

در مبحث مدیریت راهبردی دفاعی امنیتی؛ اولین مرحله از سلسله گام‌های طرح‌ریزی راهبردی دفاعی، تبیین ارکان جهت ساز می‌باشد. در جمهوری اسلامی ایران منافع ملّی سیاست‌های کلی نظام و دکترین نظامی به‌عنوان ارکان جهت ساز می‌باشند که به‌عنوان اسناد بالادستی و خطوط راهنما مبنا قرار می‌گیرند. دکترین نقش بسیار برجسته‌ای در ایجاد هماهنگی بین سازمان‌ها ایفاء می‌نماید.

۱. کلیات

۱-۱. بیان مسئله

با ایجاد فضای سایبر، بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌نمایند تا به اهداف خود در دنیای واقعی دست یابند. این اهداف از شیوه‌های متفاوتی (جنگ سایبری، تروریسم سایبری، جرائم سایبری، جاسوسی سایبری و آشفتگی سایبری و...) حاصل می‌شوند. پیشگیری، مواجهه و مقابله با این روش‌ها، برقراری امنیت در این فضا و انجام دفاع سایبری بر عهده نهادهای دفاعی- امنیتی است.

از منظر این رهاورد، حوزه‌های دفاعی امنیتی جمهوری اسلامی ایران در فضای سایبر به دلیل گستردگی و فراگیری آن، دارای شرح وظایف متنوع و بعضاً مشابهی گردیدند، لیکن به دلایل وجود فرهنگ‌های سازمانی متفاوت، شرح مأموریت خاص و اصرار بر اصل استقلال سازمانی، مدیریت راهبردی در حوزه دفاعی امنیتی دچار چالش می‌گردد. بر همین مبنا مسئولین ضمن انجام اقدامات سلیقه‌ای و موازی، ناخواسته مسبب تشدید آسیب‌ها در فرآیند دفاعی امنیتی سایبری کشور گردند. این موارد موجب نقصان در انسجام مدیریتی، یکپارچگی و وحدت رویه در بهره‌برداری از فرصت‌ها و پاسخگویی به تهدیدات فضای سایبر گردید.

عضویت برخی از نهادهای دفاعی- امنیتی در شورای عالی فضای مجازی که به تشخیص مقام معظم رهبری (مدظله‌العالی) باهدف ایجاد هماهنگی و انسجام در بین سازمان‌ها ایجاد گردیده بود، نیز رافع نواقص مدیریت راهبردی فضای سایبر در حوزه دفاعی امنیتی (متأثر از عدم هماهنگی) نگردید.

در راستای رفع این نقیصه، استفاده از دکترین مبتنی بر اصول، موجب ارتقاء سطح هماهنگی و هم‌افزایی در فرآیندهای مدیریت راهبردی و درنتیجه ایجاد وحدت و هماهنگی بیشتری می‌گردد که این امر می‌تواند در افزایش بازدارندگی در حوزه دفاعی امنیتی، تأثیرگذار باشد. تدوین دکترین حاکم بر سیاست سایبری، جمهوری اسلامی ایران را قادر می‌سازد تا راهبرد، قابلیت‌ها و وضعیت عمومی را در قبال تهدیدات سایبری تدوین و به‌طور بالقوه از این تهدیدات جلوگیری نماید. شایان‌ذکر است که بخش عمده‌ای از دکترین

که قابل بهره‌برداری توسط طراحان طرح‌های راهبردی می‌باشد را اصول و قواعد دکترینی آن، تشکیل می‌دهد.[۱]

با عنایت به موارد یادشده، می‌توان مسئله اساسی این تحقیق را چالش موجود در مدیریت راهبردی فضای سایبر جمهوری اسلامی ایران در حوزه دفاعی امنیتی ناشی از نقصان انسجام، جهت‌گیری، سیاست واحد و اتخاذ مواضع اصولی در مواجهه با مسائل آن در سطح راهبردی یاد نمود که تدوین دکترین در این حوزه امکان ایجاد وحدت رویه را فراهم می‌نماید؛ بنابراین تحقیق پیش‌رو به دنبال «تدوین اصول و قواعد دکترینی سایبری جمهوری اسلامی ایران در حوزه دفاعی- امنیتی به اقتضای ویژگی‌های ساختاری و بافتاری آن است». همچنین با توجه به ویژگی‌های خاص فضای سایبر ازجمله پویایی و پیچیدگی، مبنای فلسفی پژوهش از نوع کارکردگرایی بوده و روش پژوهش، توصیفی (اکتشافی) است.

۱-۲. اهمیت و ضرورت تحقیق

۱) مدون نمودن اصول و قواعد دکترینی سایبری موجب ایجاد وحدت رویه و افزایش هماهنگی در بخش‌های مختلف دفاعی امنیتی جمهوری اسلامی در عرصه جدید و تأثیرگذار سایبری می‌شود که نتایج آن در ارتقاء امنیت ملّی ملموس می‌باشد.

۲) تدوین اصول و قواعد دکترینی، موجب کاهش بخش عمده‌ای از ناهماهنگی‌ها و انجام اقدامات موازی و جزیره‌ای سازمان‌ها می‌شوند

۳) صرفه‌جویی در منابع و امکانات، افزایش کمیّت و کیفیت فعالیت‌های دفاعی- امنیتی در فضای سایبر از نتایج تدوین اصول و قواعد دکترینی است.

۴) این اصول علاوه بر هماهنگی، موجب استقلال سازمان‌ها در عمل نیز می‌شود.

---

۱. سایر بخش های دکترین عبارتند از استعاره دکترینی، نظریه دکترینی و فلسفه دکترینی.

۵) اصول و قواعد دکترین سایبری که بخش از دکترین سایبری هستند می‌توانند موجب ارتقاء سطح بازدارندگی در حوزه فضای سایبر گردند.

۱-۳. پیشینه تحقیق

در تحقیقات به‌عمل‌آمده، می‌توان به مقالات دکترین سیاست خارجی جمهوری اسلامی ایران بر اساس آموزه‌های قرآن، دکترین و سیاست‌های دفاعی امنیتی صحیفه سجادیه، فرایند تدوین دکترین فقهی امام خمینی(ره) در ساحت سیاست، اشاره نمود. باوجوداین به دو مورد به‌عنوان نمونه ذکر می‌گردد:

(۱) یافته‌های تحقیق خداداد هلیلی و همکاران در سال ۱۳۹۸ در مقاله‌ای با عنوان «مبانی تدوین دکترین قدرت سایبری ج.ا. ایران در سیاست‌های ابلاغی و اسناد بالادستی» حاکی از آن است که مقابله با سلطه جهانی، مواجهه هوشمندانه و تأثیرگذار در تعاملات جهانی از اصول اساسی در تدوین دکترین قدرت سایبری در سیاست‌های ابلاغی است. همچنین در اسناد بالادستی، بر شکل‌دهی به قواعد و مقررات حقوقی و قضایی سایبر و ترویج فرهنگ و ارزش‌های اسلامی تأکید شده که مبنایی برای سیاست‌ها و اهداف راهبردی در دکترین قدرت سایبری است. مقاله تبیین و تدقیق مفاهیم، شفاف‌سازی دقیق اهداف تدوین دکترین قدرت سایبری، مفهوم‌سازی معیارهای بومی سنجش و ارتقاء قدرت سایبری (نفوذ، مشروعیت، کارآمدی و بازدارندگی) و تحلیل و واکاوی جریان‌های فکری مسلط و تأثیرگذار فضای سایبر بر دکترین و مطالعه تطبیقی دکترین قدرت سایبری در سایر کشورها را در مفهوم‌سازی تدوین دکترین قدرت سایبری حائز اهمیت می‌داند.

(۲) اندیشکده امریکن اینترپرایز در سال ۲۰۱۷ پژوهشی تحت عنوان «دیدگاه‌های ایران درباره جنگ: درک دکترین‌های در حال تحول تهران» منتشر نموده که ماهیت دکترین‌های جمهوری اسلامی ایران را تدافعی با چهار هدف اصلی امنیت

ملّی، دفاع سرزمینی، بازدارندگی نمایش محور (نمایش قدرت) و بازدارندگی تلافی‌جویانه اعلام می‌نماید. در جدول یک، دکترین‌های دو حوزه زمینی و سایبری عنوان‌شده است.

جدول ۱- دکترین‌های دفاعی – امنیتی جمهوری اسلامی ایران از منظر اندیشکده امریکن اینترپرایز

دکترین و توانایی‌های در حال ظهور		دکترین و توانایی‌های توسعه‌یافته		
پروژه قدرت اجباری	صدور انقلاب و نفوذ ج.ا.ا	بازدارندگی تلافی‌جویانه	بازدارندگی نمایشی	دفاع سرزمینی
جنگ سایبری	پشتیبانی سایبری از جنگ نامتعارف	تلافی سایبری		دفاع سایبری

(۳) ولوی و مرادی در سال ۱۳۹۹ در مقاله ای با عنوان فلسفه فضای سایبری جمهوری اسلامی ایران چیست بیان می دارند که در کشورهای تابع فناوری، جذابیت و اغواگری فضای سایبر با یک عقبه نظامی باعث شده که غالباً به لایه‌های فوقانی و جنبه‌های ظاهری آن پرداخته شود و درنتیجه عدم توجه به فلسفه و ماهیت وجودی آن در کوتاه‌مدت غافلگیری راهبردی حاصل گردد.با توجه به این‌که فضای سایبر درشاکلهٔ خود واجد جهت‌گیری‌های زیادی است ازاین‌رو ضرورت تأمل در خصوص فلسفه وجودی فضای سایبری ج.ا.ایران احساس می‌شود.یافته این پژوهش این است که از آن جایی که تسلط اصول مدرنیسم در فضای مجازی مطلق نبوده لذا شورش علیه ایدئولوژی فضای مجازی و تغییر در آن ممکن می‌باشد بنابراین باید ضمن به رسمیت شناختن آن و کاهش حداکثری سلطه همه‌جانبه آن بر زندگی بشر، این فضا را بر مبنای وحی پایه‌ریزی و بومی کنیم.

(۴) دانش آشتیانی در سال ۱۳۸۸ در مقاله ای با عنوان اصول و روش تدوین رهنامه نظامی چگونه است؟ بیان می نماید که رهنامه ماهیتاً از جنس اندیشه و تفکر است که اصالتاً در تفکر و جهان‌بینی و قالب‌های ذهنی افراد ریشه دارد و معمولاً به‌صورت نظریه اعلان می‌شود. به‌طورکلی رهنامه را می‌توان به دو نوع فردی و

سازمانی تقسیم‌بندی کرد. افراد اعم از رهبران، فرماندهان نظامی، مدیران یا کارکنان سازمان‌ها در هر سطحی معمولاً برای تصمیم‌گیری، اجرای مأموریت و انجام امور، دارای رهنامه خاص خود می‌باشند از طرفی رهنامه سازمانی و ملّی که از نوع فرایند شبیه هم هستند، هنگامی شکل می‌گیرند که در سازمان یا در سطح ملّی برای اجرای یک وظیفه خاص یا یک مأموریت، رهنامه فردی یک مدیر پذیرفته می‌شود یا در مورد رهنامه‌های فردی مدیران سازمان اجماع حاصل می‌شود. در این تحقیق رهنامه نظامی یا رهنامه سازمانی و رسمی نیروهای مسلّح به سه نوع رهنامه نیرویی، رهنامه مشترک و رهنامه مرکب تقسیم می‌شود و دارای سه سطح راهبردی، عملیاتی و تاکتیکی است.

۱-۴. سؤال‌های تحقیق

۱-۴-۱. سؤال اصلی

اصول و قواعد دکترین سایبری ج.ا.ایران در حوزه دفاعی امنیتی چیست؟

۱-۴-۲. سؤال‌های فرعی

(۱) اصول دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی چیست؟

(۲) قواعد دکترینی سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی چیست؟

۱-۵. هدف‌های تحقیق

۱-۵-۱. هدف اصلی

تدوین اصول و قواعد دکترین سایبری ج.ا.ایران در حوزه دفاعی امنیتی

۱-۵-۲. هدف‌های فرعی

(۱) تدوین اصول دکترینی سایبری جمهوری اسلامی ایران در حوزه دفاعی- امنیتی.

(۲) تدوین قواعد دکترینی سایبری جمهوری اسلامی ایران در حوزه دفاعی- امنیتی.

۱-۶. روش‌شناسی تحقیق

پژوهش حاضر، پژوهشی توسعه‌ای-کاربردی است زیرا این پژوهش، مبادی شناختی خود را از مبانی فلسفی، نظریه‌ها، قوانین و نتایج پژوهش‌های بنیادی می‌گیرد (توسعه‌ای) و با شناسایی عوامل و مبانی تدوین دکترین سایبری و درنهایت ارائه اصول دکترین سایبری منجر به جهت‌گیری و اتخاذ مواضع اصولی در حوزه دفاعی امنیتی فضای سایبر در کشور می‌گردد، یک پژوهش کاربردی است. پژوهش حاضر ازلحاظ رویکرد تحقیق در زمره تحقیقات کیفی دسته‌بندی می‌شود. پژوهش‌های کیفی نقش اکتشافی دارند. به‌صورت کلی روش‌های تحقیق زیر در این مقاله استفاده‌شده است.

۱. **اکتشافی:** با روش کیفی، ادبیات تحقیق بررسی‌شده است.
۲. **مورد پژوهی:** مشاهده تفصیلی ایجاد یک پدیده مطالعه و تفسیر آن‌ها برای رسیدن به درکی عمیق از دیدگاه کل گرا
۳. **تحلیل مضمون:** برای بررسی محتوای آشکار پیام‌های موجود در متون از این روش استفاده‌شده است.
۴. **مصاحبه عمیق:** در جهت تکمیل و رفع نقصان در ادبیات تحقیق با خبرگان حوزه دکترین و فضای سایبر مصاحبه عمیق به عمل آمد.
۵. **مصاحبه کانونی:** در راستای جمع‌بندی تعاریف عملیاتی و بومی پژوهش جلساتی به‌منظور بهره‌مندی ازنظرات خبرگان تشکیل گردید.

در این تحقیق، مبانی نظری و منابع به‌دست‌آمده شامل اسناد حکومتی، مذهبی، سازمانی و علمی در ادبیات تحقیق با استفاده از نرم‌افزار maxqda2020 طی سه مرحله کدگذاری (باز، محوری، انتخابی) شد که حاصل آن احصاء،۲۲۴ کد بود. سپس این کدها با توجه مفاهیمی که داشتند در محورهای جداگانه طبقه‌بندی گردیدند و در نهایت در بخش کدگذاری انتخابی ۱۷ مفهوم (طبقه) به دست آمد که این مفاهیم به‌عنوان قواعد دکترینی سایبری در حوزه دفاعی امنیتی، نامیده شدند. شیوه دسته‌بندی این کدها در با استفاده از تعاریف فضای سایبر ازجمله حوزه شناختی، اطلاعاتی، فیزیکی، سایبر در رزم، رزم سایبری، حکمرانی سایبری، امنیت سایبری و همچنین اصول ارزشی جمهوری اسلامی

ایران از قبیل عدالت محوری، اخلاق‌مداری و... صورت گرفت. سپس این مفاهیم مجدداً طبقه‌بندی گردید که شامل سه دسته قواعد در جهت حفظ موجودیت انقلاب اسلامی، حفظ حاکمیت انقلاب اسلامی و حفظ هویت انقلاب اسلامی در راستای مقابله با تهدیدات سخت، نیمه سخت و نرم گردیدند. عنوان هرکدام از این دسته‌ها به‌عنوان اصول دکترینی سایبری قلمداد شدند.

جامعه آماری اسناد مشتمل بر منابع علمی داخلی و خارجی، اسناد و منابع علمی معتبر داخلی و خارجی در حوزه دکترین، سایبر و دفاعی امنیتی است که از شیوهٔ نمونه‌گیری هدفمند استفاده‌شده است. روش گردآوری داده‌ها به روش کتابخانه‌ای به‌وسیله پیمایش اسناد با ابزار فیش‌برداری است.

انتخاب جامعه آماری خبرگان به‌صورت نمونه‌گیری هدفمند و با مشورت صاحب‌نظران حوزه دکترین، فضای سایبر و دفاع و امنیت بوده است و به روش گلوله برفی انجام‌شده است. لیکن پس از انجام مصاحبه عمیق با برخی از خبرگان و به‌منظور افزایش دقت و کیفیت مطالب، از کتاب‌ها و مقالات و نوشته‌های همان خبره استفاده شد به‌عبارت‌دیگر انجام مصاحبه به‌منظور مفاهمه بیشتر واژه‌ها و فرآیندها صورت پذیرفته است.

مصاحبه گروه کانونی نیز به‌منظور جمع‌بندی تعاریف به‌دست‌آمده، با چهار نفر از اساتید صاحب‌نظر دانشگاه (با مدرک دکتری) که دارای تجربیات عملی درزمینه تدوین دکترین و دارای کتاب و مقاله در این حوزه بودند انجام شد. قلمرو موضوع این تحقیق در حوزه فضای سایبری دفاعی و امنیتی می‌باشد و قلمرو جغرافیایی آن، جغرافیای مؤثر بر امنیت ملّی جمهوری اسلامی در فضای سایبری می‌باشد. قلمرو سازمانی این تحقیق نیروهای مسلح جمهوری اسلامی ایران می‌باشد.

۱-۷. پایایی و روایی تحقیق

در پژوهش‌های کیفی نحوه محاسبه روایی و پایایی با پژوهش‌های کمی متفاوت است. از دیدگاه کرسول[1] برای نیل به روایی پژوهش کیفی از معیارهایی مانند تماس طولانی با فضای پژوهش، مشاهده مستمر، بررسی از زوایای مختلف، تحلیل موارد منفی، گردآوری از منابع اطلاعاتی متنوع، بررسی کردن تفاسیر در مقابل داده‌های خام، تبادل‌نظر با همتایان و کنترل بیرونی از طریق شخص ثالث یا داور می‌توان استفاده کرد (کرسول، ۲۰۱۴). برای بررسی پایایی پژوهش نیز از ضریب کاپای کوهن[2] استفاده می‌شود. مقادیر بالای ۰/۶ پایایی پژوهش را نشان می‌دهد. از سوی دیگر محققین برای پایایی اسناد و مدارک تحقیق اقدام به مستند نمودن آن‌ها نموده‌اند؛ و برای روایی اسناد و مدارک، محققین اقدام به جمع‌آوری داده‌ها از چندین منبع مختلف و تطبیق و مقارنه آن‌ها پرداخته‌اند که برای نمونه به مقاله ایجاد دکترین جنگ سایبری و همچنین پژوهش‌های منابع معتبر داخلی و پژوهشکده امریکن اینترپرایز اشاره نمود.

۲. ادبیات و مبانی نظری تحقیق

در حوزه امنیت و دفاع سایبری تعیین رویکرد و نحوه مواجهه ارکان یک کشور با این فضا در سایر تصمیمات پیرامونی بسیار تأثیرگذار است. مع‌الوصف تدوین دکترین به‌عنوان یکی از گام‌های برنامه‌ریزی راهبردی در خصوص موضوع فی‌الذاته پیچیده‌ای چون فضای سایبر مطرح است.

۲-۱. تعاریف

(۱) **اصول:** مجموعه‌ای از ارزش‌ها و قواعد بنیادین پایدار که بر کلیه تصمیمات و اقدامات حاکم است و هدایت‌گر تدوین سیاست‌ها راهبردها برنامه‌ریزی‌ها و امور اجرایی برای نیل به اهداف تعیین‌شده می‌باشد. (ستاد کل نیروهای مسلّح،۱۳۸۹؛۲).

---

۱. Creswell
۲. Cohen's Kappa Coefficient

(۲) **دکترین:** اصول و قواعدی است که در یک علم خاص و به‌منظور هـدایت‌گـری و کاربست عملی به کار می‌رود. (محققین)

(۳) **دکترین سایبری:** 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.(محققین)

(۴) **حوزه دفاعی امنیتی:** دفاعی است مبتنی بر امنیت ملـی و یکپـارچگی مؤلفـه‌هـای قدرت ملی یا به‌عبارتی‌دیگر، دفـاع یکپارچـه‌ای کـه امنیـت ملـی نسـبی را تـأمین کند.(تقریرات درسی دکتر توحیدی، ۱۳۹۳)

(۵) **سایبرنتیک:**[۱] واژه پرکـاربرد حـوزه کنتـرل و ارتباطـات در نیمـه دوم قـرن بیسـتم میلادی است. این واژه از لغـت یونـانی Κυβερνήτης بـه معنـای سـکان‌دار والـی اخذشده است.[۲](کیانخواه، ۱۳۹۷:۷)

(۶) **فضای مجازی (سایبر):** فضای مجازی، امتزاجی از فضای حقیقی است و به ابزاری جهـت بسط و تحکیم حاکمیت ملّی در مناسبات جهانی و کشوری مبدل شده است (محققین).

(۷) **قاعده:** قاعده ازنظر لغوی به معنای بنیان، اساس و ... اسـت. ازنظـر لغـوی گـاهی قاعده و اصل مترادف هم هستند؛ اما در ترکیب اصطلاح « قاعدهٔ حقوقی » قاعـده به معنای قانون و یا حکم عام است. ازنظر اصـطلاحی، قواعـد حقـوقی، احکـامی کلی، الزام‌آور و دارای ضمانت اجرا هستند که از سوی مرجعی ذیصلاح، به‌منظور ایجاد نظم در روابط اجتماعی وضع می‌گردند. (کاتوزیان، ۱۳۸۸؛ ۵۱۶)

(۸) **قواعد دکترینی:** الگوهـا، ضـوابط، چـارچوب‌هـا، ابتکـارات و روش هـای کلـی استانداردی است که با هدف ایجاد هماهنگی بین یگان های مختلف عمـل کننـده تدوین می شود. (ستاد کل نیروهای مسلّح،۱۴۰۱؛۲۳۰).

---

۱. Cybernetics

۲. لفظ Governor به معنای فرماندار با سایبرنتیک هم‌ریشه است.

(۹) **مدیریت راهبردی دفـاعی- امنیتـی:** نظـام جـامع طـرح‌ریـزی، برنامـه‌ریـزی و بودجه‌بندی از دهۀ ۶۰ قرن بیستم در نیروهای مسلّح هم‌زمان و همگام بـا نظریـه، مدیریت راهبردی، به مرحله اجرا درآمد. ایـن نظـام اکنـون پـس از سـیر مراحـل تکوینی و تکمیلی خود در پارادایم تلفیقی، تحت عنوان نظام مـدیریت راهبـردی دفاعی- امنیتی بهینه‌شده و در کشورهای مختلف جهـان، بـا یـک فرآینـد تقریبـاً مشابه، پذیرفته و به مرحله اجرا درآمده است. (دانش آشتیانی، ۱۳۹۰، ۱۱۴)

۲-۲. مفروضات اساسی

۲-۲-۱. نظریات

بررسی کلی رویکردهای توسعه غربی نشان می‌دهد که فناوری نقش اساسی در تـدوین نظریـات توسـعه‌ای دارد بـه‌عبـارت‌دیگـر رویکردهـای جدیـد توسـعه، موجـب تغییـر جهت‌گیری‌های فناوری می‌شود. به‌صورت مشخص نظریه نظام جهانی بـر انجـام پیشـرفت به‌صورت شبکه‌ای و در سطح بین‌الملل تأکید دارد به‌نحوی‌که شبکه‌هـا و سـاختارهای بـاز بدون هیچ محدودیتی می‌توانند گسترش یابند و این امر زمانی میسر اسـت کـه ایـن نقـاط، توانایی ارتباط در شبکه را داشته باشند. این نظریه تا جایی پیش می‌رود کـه واحـد تحلیـل کشور-ملت را به‌نظام بین‌الملل تغییر می‌دهد. فضای سایبر با کلیه خـدمات شـایانی کـه بـه بشر می‌نماید بستر و زیرساختی است برای پیاده‌سازی اهدافی که توسـط حاکمـان فنـاوری برای جهان ترسیم‌شده است. اصل انقلاب اسلامی ناظر بر سه رکن اساسی متجلی می‌گـردد به‌گونه‌ای که حفظ انقلاب اسلامی مستلزم پایـداری هـر سـه رکـن مـی‌باشـد. ایـن ارکـان عبارت‌اند از:

۱. موجودیت انقلاب اسلامی در برابر تهدید سخت

۲. حاکمیت انقلاب اسلامی در برابر تهدید نیمه سخت

۳. هویت انقلاب اسلامی در برابر تهدید نرم. (مرادی قاسم‌آبادی، ۱۳۸۷: ۳۴)

۲-۲-۲. فلسفه تکنولوژی[۱]

بشر برای رفع بسیاری از مشکلات خود به ساختن تکنولوژی روی آورده است. تکنولوژی اگرچه در حل بسیاری از چالش‌ها مؤثر بوده لیکن تأثیراتی بعضاً شگرف بر انسان می‌گذارد و قادر است در میان افراد و جامعه تغییراتی گوناگون ایجاد نماید، همچنین تکنولوژی منشأ برخی از مشکلات نیز برای انسان گردیده است.

۲-۲-۳. فضای سایبر

فضای سایبر؛ بانفوذ گسترده خود در تمامی ابعاد زندگی بشر، معادلات و مناسبات بین‌المللی را دستخوش تغییر نموده و شکل جدید و متفاوتی از قدرت را بر مبنای تعاملات اقتصادی، تجاری، فرهنگی و اجتماعی و جهانی‌شدن به وجود آورده است تبدیل فضای سایبر به میدان پنجم نبرد بعد از عرصه‌های زمین، دریا، هوا و فضا نشان‌دهنده پویایی فضای سایبر و چالش‌های ناشی از جنگ‌های سایبری است (عباسی، بابایی، شامحمدی، ۱۳۹۲).

۲-۲-۴. دفاع و امنیت سایبری

فضای سایبر بر نوع و کیفیت دفاع و امنیت تأثیر دارد و متقابلاً فضای سایبر نیاز به دفاع و امنیت دارد. وجود فضای سایبر ملاحظات و ترتیبات جدیدی در ابعاد ساختاری، رفتاری، بافتاری و محتوایی بر دفاع و امنیت تحمیل می‌کند و فضای سایبر هم برای پایداری و قابلیت اطمینان، نیازمند راهبردها و اقدامات خاص دفاعی امنیتی است. مواردی که در این مقوله به آن پرداخته می‌شود عبارت‌اند از: واژه دفاع در بیانات مقام معظم رهبری، جنگ اطلاعاتی، قدرت سایبری، دفاع سایبری، جنگ سایبری، امنیت سایبری، بازدارندگی سایبری.

---

۱. در این مقاله از بعضی از واژه‌های لاتین استفاده‌شده، درصورتی‌که فرهنگستان زبان فارسی، برای آن‌ها معادل فارسی اعلام نموده است که این امر دو دلیل داشته است. دلیل اول، این مقاله به بررسی ماهیت و ریشه واژه‌هایی مثل تکنولوژی می‌پردازد (تخنه)، بنابراین استفاده از واژه‌های جایگزین گویای مسئله نیست. دلیل دوّم، در منابع اقتباس‌شده این کلمات دقیقاً به همین شکل استفاده‌شده است.

۲-۳. دکترین

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 به واسطه‌ای دارد. بر این اساس، دکترین موضوعیت پیدا می‌کند تا غبار ابهام را از چهره آن بزداید و بتواند به سیاست‌های مشخصی جهت اداره انسان تبدیل شود. (سید رحمانی، ۱۳۹۳)

۲-۳-۱. تعاریف دکترین: ازنظر لغوی، دکترین در فرهنگ لغات فارسی با واژه‌هایی مانند مسلک، عقیده، رأی، نظریه و فکر (فرهنگ عمید: ۱۱۳۴) مترادف است. از منظر مقام معظم رهبری (مدظله‌العالی)، دکترین مفهومی بنیانی و راهبردی است و چیز تاکتیکی نیست.(مع ط.ب.ب س.ک.ن.م،۱۳۸۹). به معنای اصول بنیادین، باورها و چارچوب‌های نظری، دیدگاه، الگو، خط‌مشی، چگونگی عمل، راهنما و روش است. (ثروتی، مظلوم،۱۳۹۱) در برخی منابع نیز از واژه «رهنامه» به‌عنوان معادل فارسی دکترین استفاده و این تعریف برای آن ارائه‌شده است: رهنامه مجموعه‌ای از اصول و قواعد اساسی است که به‌واسطه نظر خبرگان مرتبط با اولویت‌بندی مناسب کنار هم قرار می‌گیرند (افشردی و همکاران، ۱۳۹۶).

۲-۳-۲. ملزومات تدوین دکترین: اصول بنیادین و قواعد پایه دکترین ریشه در ارزش‌ها و هنجارهای ملّی دارد. به‌عنوان‌مثال، از دیدگاه خلیلی، تدوین دکترین امنیت ملّی، در قالب مثلثی از اهداف و آرمان‌های ملّی، ارزش‌ها و هنجارهای ملّی و منافع و مصالح ملّی امکان‌پذیر است که اهداف و آرمان‌های ملّی در رأس این مثلث قرار دارند باوجوداین دکترین امنیت ملّی حاصل جمع و برآیند هر سه عنصر است که در کنار یکدیگر ترسیم‌کننده وضعیت مطلوب برای هر کشور هستند (خلیلی، ۱۳۸۶:۴۴۱). هنگامی‌که 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. (دانش آشتیانی، ۱۳۸۸: ۵۶).

۲-۳-۳. رابطه دکترین، سیاست و راهبرد: برای تبیین درست میان دکترین، سیاست و راهبرد در گام اول لازم است به درکی مستقل از مفهوم امنیت دست‌یابیم. باوجوداین رابطه‌ای

سلسله مراتبی میان دکترین، سیاست و استراتژی برقرار است. دکترین به دلیل این‌که ماهیت هدف‌گذاری دارد در رأس قرارمی‌گیرد. پس‌ازآن سیاست است که بیانگر هدایت امکانات موجود در راستای هدف است و درنهایت راهبرد قرار دارد که چگونگی به‌کارگیری امکانات موجود برای تحقق اهداف است. (خلیلی، رضا،۱۳۸۶: ۴۴۵).

۲-۳-۴. منابع ورودی تدوین دکترین: طی مصاحبه کانونی که توسط محققین با جمعی از خبرگان برگزار شد، منابع ورودی تدوین دکترین سایبری عبارت شدند از منابع مذهبی (قرآن کریم، بیانات مقام معظم رهبری) حکومتی (اوامر حکومتی مقام معظم رهبری، قانون اساسی، احکام شورای عالی فضای مجازی)، سازمانی (چشم‌انداز و بیانیه س.ک.ن.م) و علمی (مقاله‌ها و رساله‌ها). در همین راستا محققین به بررسی اسناد به شرح زیر اقدام نمودند، هرچند تعداد اسناد بررسی‌شده بیش از موارد یادشده می‌باشند (ازجمله سیاست‌های کلی نظام در حوزه‌های دفاعی امنیتی)

جدول ۲- اسناد بالادستی تدوین قواعد دکترینی

ردیف	نام سند	نوع منبع
۱	قرآن کریم	مذهبی
۲	قانون اساسی جمهوری اسلامی ایران	حکومتی
۳	حکم انتصاب اعضای جدید شورای عالی فضای مجازی	حکومتی
۴	بیانیه ستاد کل ن.م در حوزه تهدیدات سایبری	سازمانی
۵	چشم‌انداز نیروهای مسلح جمهوری اسلامی ایران	سازمانی
۶	بیانیه گام دوم انقلاب اسلامی	حکومتی
۷	چشم‌انداز ۱۴۰۴ جمهوری اسلامی ایران	حکومتی
۸	بیانات مقام معظم فرماندهی کل قوا در حوزه سایبری و جنگ نرم	حکومتی
۹	اسناد حاکمیتی فناوری اطلاعات و ارتباطات سایبری	حکومتی
۱۰	دکترین‌های دفاعی امنیتی	علمی
۱۱	اصول راهبردی حاکم بر حکمرانی سایبری ج.ا.ا	علمی
۱۲	سیاست‌های مقابله با تهاجم فرهنگی و ناتوی فرهنگی در کلام رهبری	حکومتی
۱۳	سیاست‌های کلی نظام	حکومتی
۱۴	سند تبیین الزامات شبکه ملّی اطلاعات	حکومتی
۱۵	طرح کلان و معماری شبکه ملّی اطلاعات	حکومتی
۱۶	سند جامع علم و فناوری در حوزه دفاعی و امنیتی ج.ا.ا	سازمانی

۲-۳-۶. مدل‌های تدوین دکترین: طبق بررسی‌های به‌عمل‌آمده تاکنون جهت تدوین دکترین سایبری در جمهوری اسلامی ایران روش منتشرشده‌ای وجود ندارد لیکن چند نمونه از روش‌های متداول تدوین دکترین است که قابلیت بهره‌برداری به‌عنوان مبنایی جهت تدوین دکترین سایبری قرار گیرد به شرح زیر بررسی می‌گردد:

(۱) **مدل سیستمی**: این مدل توسط هیئت عالی آئین‌نامه‌های ن.م ارائه‌شده است.(ثروتی،۱۳۹۱).

(۲) **مدل دکترین نظامی**: یک روش پنج مرحله‌ای برای تدوین دکترین نظامی شامل شناسایی مناقشه و ماهیت آن؛ بررسی نقطه نظرات دشمن؛ توسعه راهبرد ملّی؛ توسعه راهبرد نظامی؛ توسعه و تدوین دکترین نظامی (دانش آشتیانی، ۱۳۸۸: ۶۰)

(۳) **مدل** تدوین دکترین در روسیه: 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 شرق دکترین برداشت مشترکی از مطالبات دفاعی ملّی است. (موسسه آموزشی و تحقیقات صنایع دفاعی، ۱۶:۱۳۸۶)

۲-۴. دفاع و امنیت در جمهوری اسلامی ایران

به همان اندازه که جنگ عملی ناخوشایند و ناپسند است، دفاع امری عقلانی و پسندیده است. مقام معظم رهبری دراین‌باره فرمودند: دفاع جزئی از هویت یک ملت زنده است. هر ملتی که نتواند از خود دفاع بکند، زنده نیست. هر ملتی هم که به فکر دفاع از خود نباشد و خود را آماده نکند، درواقع زنده نیست. هر ملتی هم که اهمیت دفاع را درک نکند، به یک معنا زنده نیست {بنابراین} ما دفاع مشروع را حق خود می‌دانیم {چراکه} تنها چیزی که می‌تواند کشور ایران و نظام اسلامی را حفظ کند استحکام داخلی و عزم جزم بر دفاع مشروع و منطقی است (بیانات مقام معظم رهبری(مد ظله‌العالی) پس از بازدید از ستاد کل سپاه پاسداران انقلاب اسلامی رهبری؛ ۶۸/۸/۲۹).

«**حیات جهادی» رهبر انقلاب اسلامی**: معظم له حیات جهادی خود را با دو مشخصه‌ی «مقاومت» و «تبیین» معرّفی می‌کنند و البته تصریح می‌فرمایند که «مبارزه‌ی بدون روشنگری منجر به ارتجاع» و «روشنگری بدون مبارزه به پوچی» می‌انجامد. (صلح میرزایی،۱۴۰۰: ۵)

در این مقوله بحث‌های زیر قابل‌بررسی است: رویکرد تهدید در مقابل تهدید، قدرت بازدارندگی در بیانات مقام معظم رهبری(مد ظله‌العالی)، قانون اساسی، سیاست‌های کلان کشور، مؤلفه‌های بازدارندگی ج.ا.ا، امنیت فضای سایبر جمهوری اسلامی ایران.

۲-۵.ارکان جهت ساز دکترین سایبری ج.ا.ا

موضوع تدوین دکترین سایبری، مستلزم شناخت مؤلفه‌های مرتبط با آن در سیاست‌های ابلاغی، قانون اساسی و اسناد بالادستی این حوزه است. در این بخش، مروری بر فرمان‌ها و رهنمودهای مقام معظم رهبری (مدظله‌العالی) و اسناد بالادستی که مهم‌ترین عوامل مؤثر در نحوه تدوین ارکان دکترین سایبری هستند؛ می‌پردازیم.

مروری بر بیانات مقام معظم رهبری (مدظله‌العالی) در حوزه قدرت و قدرت ملّی، سیر تکامل نظریات ایشان از منابع و ابزارهای قدرت سنتی به قدرت سایبری را نشان می‌دهد؛ بنابراین مفهوم‌سازی و تبیین دکترین این چهره نوین از قدرت، برای تدوین راهبردها و در پیش گرفتن رویکردهای مناسب، در راستای عمل به رهنمودها و سیاست‌های کلان ابلاغ‌شده توسط معظم له امری ضروری به نظر می‌رسد. ازآنجاکه گفتمان و بیانات داهیانه رهبر معظم انقلاب مبتنی بر اجتهاد و اشراف بر مبانی فقهی و قرآنی و تجربیات چندین ساله معظم له در هدایت و راهبری نظام اسلامی است لذا تبلور عینی و عملیاتی دکترین سایبری نیز باید مبتنی بر منظومه فکری معظم له، طرح‌ریزی و اجرا گردد.

۲-۵-۱. تعدادی از فرامین و رهنمودهای مقام معظم رهبری(مدظله‌العالی)در بیانات و دیدارهای زیر به شرح زیر می‌باشند:

۱. حالا که دیگر فضای مجازی هم است؛ یک دستگاهِ بی در و دروازه که هر کس هر چه دلش می‌خواهد می‌نویسد. (رئیس و مسئولان قوه قضائیه ۹۸/۰۴/۰۵)

۲. دشمن ازلحاظ فضای مجازی آرایش جنگی گرفته؛ در مقابل این دشمنی که آرایش جنگی در مقابل ملّت ایران گرفته، ملّت ایران بایستی آرایش مناسب بگیرد، باید خودش را آماده کند در همه‌ی بخش‌های مختلف. (معلمان و فرهنگیان-۹۸/۰۲/۱۱)

۳. مرزبندی با دشمن برای مصونیت از تهاجم نرم [است]. یکی از کارهای بسیار لازم همین است که ما نگذاریم مرزمان با دشمن کم‌رنگ بشود؛ درست مثل مرزهای جغرافیایی. (فرماندهان نیروی انتظامی – ۹۸/۰۲/۰۸)

۴. از این فضا (مجازی)، دشمن علیه هویت شما، موجودیت شما، نظام شما، انقلاب شما استفاده نکند. (اعضای شورای هماهنگی تبلیغات اسلامی- ۹۶/۱۰/۰۶)

۵. یکی دیگر از چیزهایی که در مدیریت کشور -که بتوانید کشور را اداره کنید- تأثیر دارد، مسئله‌ی فضای مجازی است. (دیدار مسئولان نظام ۹۶/۰۳/۲۲)

۶. جنگ نرم یک عرصه‌ی بسیار وسیعی است و روزبه‌روز هم با گسترش این فضای مجازی دارد گسترده‌تر می‌شود و خیلی هم خطرناک‌تر از جنگ سخت است(بسیجیان ۹۵/۰۹/۰۳)

۷. در بین مسئولین هم هستند کسانی که اهمّیّت این کار بزرگ (فضای مجازی) را به‌درستی و آن‌چنان‌که بایدوشاید درک نمی‌کنند لذا اقدام لازم را انجام نمی‌دهند.(درس خارج فقه ۹۵/۰۶/۱۶)

۸. انواع جنگ نرم: ۱- تحریم اقتصادی، تبلیغات اغواگر ۲- زدن عقبه‌های جمهوری اسلامی در برخی از کشورهای دیگر ۳-نفوذ برای تغییر باورهای مردم (اعضای مجلس خبرگان رهبری ۹۵/۰۳/۰۶)

۹. این میدان (فضای مجازی)، میدان واقعی جنگ است. (حوزه‌های علمیه ۹۵/۰۲/۲۵)

۱۰. ابزارهای تسهیل‌کننده، مثل فضای مجازی و سایبری هم که الان در اختیار شماست. اگر بتوانید این‌ها را یاد بگیرید، می‌توانید یک کلمه حرف درستِ خودتان را به هزاران مستمعی که شما آن‌ها را نمی‌شناسید، برسانید؛ (علما و روحانیون خراسان شمالی ۹۱/۰۷/۱۹)

۲-۵-۲. ده استنباط از دیدگاه‌های مقام معظم رهبری(مدظله‌العالی)

(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 ملّی در مناسبات جهانی و کشوری.

(۶) چالش دوقطبی سازی سیاسی کاذب در توسعه کشور.

(۷) چالش تسلط کمپانی‌های بزرگ تحت سلطه آمریکا.

(۸) چالش شکاف توسعه در مقایسه با روند پیشرفت و شتاب فناوری.

(۹) توان و ظرفیت زیرساختی بالقوه (مردم- نخبگان- فناوری- ساختار- اقتصاد و...).

(۱۰)ضرورت تدوین نقشه راه حکمرانی در فضای مجازی (ولوی، ۱۳۹۹: ۳)

۲-۵-۳. برخی از اصول راهبردی حاکم بر حکمرانی جمهوری اسلامی در فضای مجازی که ناظر به تفکر کلان جمهوری اسلامی ایران در مواجهه با فضای مجازی است را در قالب اصول زیر می‌توان بیان نمود:

(۱) فرصت نگری به فضای مجازی.

(۲) صیانت از مرزهای ملّی و دینی.

(۳) حمایت از حقوق و آزادی‌های مشروع مردم در فضای مجازی.

(۴) مواجهه فراملی با فضای مجازی.

(۵) سلطه گریزی و عدالت‌طلبی در فضای مجازی.

(۶) تبدیل‌شدن به بازیگری مؤثر در فضای مجازی بین‌المللی.

(۷) مردم‌گرایی در فضای مجازی.

(۸) اخلاق‌گرایی و صیانت از کرامت انسانی در فضای مجازی.

(۹) محوریت پیام در فضای مجازی.

(۱۰)تعامل و همکاری با کشورها و ملت‌های همسو (غلامی، ۱۳۹۸)

۲-۶. محیط سایبری دفاعی امنیتی جمهوری اسلامی ایران

دکترین‌ها، در طول تاریخ دستخوش تغییر و تحول شده و این تغییرات به‌ویژه تحت تأثیر پیشرفت‌های علمی، فناوری، تسلیحاتی، تغییرات محیطی و نوع و ماهیت تهدیدات بوده است. در این بخش به بررسی محیط سایبری دفاعی امنیتی ج. ا.ایران می‌پردازیم.

۱-۶-۲. ساختار دفاعی امنیتی سایبری در ایران

با توجه به ویژگی‌های فضای سایبر و توانمندی‌ها و اقدامات دشمنان نظام مقدس جمهوری اسلامی ایران در این حوزه و همچنین شرایط کشور در همه ابعاد حوزه سایبر، به‌صورت کلی وضعیت سایبری کشور را به شرح جدول ۳ می‌توان تحلیل نمود. (دانشگاه جامع امام حسین(ع)، ۱۳۹۷: ۴۷-۴۵)

جدول ۳- وضعیت سایبری ج.ا.ا

حوزه	ملاحظات
تدبیر فرماندهی	فرامین و فرمایشات متعدد از سوی مقام معظم رهبری (مدظله‌العالی) در خصوص اهمیت فضای سایبر و توجه به تهدیدات و آسیب‌پذیری‌های آن و لزوم مصونیت بخشی آن وجود دارد.
محیط عملیاتی	از فضای سایبر می‌توان به‌عنوان یک مزیت برتر ساز عملیاتی در سطح ن.م. بهره‌گیری نمود.
قدرت تولید تهدید	تهدید در برابر تهدید دشمن و حمله در برابر حمله دشمن به‌راحتی امکان‌پذیر است.
قدرت نامتقارن	امکان ایجاد قدرت نامتقارن مبتنی بر جنگ سایبری در جنگ‌های نامتقارن وجود دارد.
بازدارندگی	قدرت سایبری می‌توان جایگزین قدرت هسته‌ای در جهت بازدارندگی در هر کشوری شود.
حکمرانی جهانی	راهبرد آمریکا اداره جهان از طریق سایبر است.
قطعات سامانه‌ها	هر قطعه الکترونیکی در سامانه‌ها یک نقطه ممکن برای ورود به آن سامانه‌ها است.
فناوری‌های نوظهور	این فناوری‌ها (هوش مصنوعی و..) شرایط امنیتی آینده جهان و کشور را متحول خواهند کرد.
ائتلاف‌های بین‌المللی	این ائتلاف‌ها در حوزه تأمین امنیت سایبری بین کشورهای استکباری در حال گسترش است

۲-۶-۲. نقاط ضعف سایبری دفاعی امنیتی ج.ا.ا

امکان ارائه به دلیل مطالب طبقه بندی شده وجود ندارد

۲-۶-۳. نقاط ضعف سایبری دشمن

باوجود توانمندی‌های زیادی که از طریق فضای سایبر برای دشمنان جمهوری اسلامی ایران به وجود آمده است لیکن دارای نقاط ضعفی نیز در این حوزه هستند که اهم آن به شرح زیر است:

(۱) گسترش بیش‌ازاندازه نیروهای آمریکایی در سطح دنیا

(۲) وابستگی فناورانه و آسیب‌پذیری‌های ناشی از آن

(۳) پایین بودن آستانه تحمل دشمن در مقابل افزایش زمان، هزینه و تلفات

(۴) آسیب‌پذیری‌های سایبری و شبکه‌ای

(۵) هزینه‌های بالای نظامی (شامحمدی، ۱۳۹۳: ۱۱۳)

۲-۶-۴. آینده فضای سایبر

پنج آیندهٔ سایبری بالقوه مجموعه‌ای از محیط‌های سایبری را که ممکن است تا سال ۲۰۵۰ شکل گیرند تعریف می‌کنند. این آینده‌ها عبارت‌اند از:

– **وضعیت کنونی**: نبرد سایبری آتی شبیه نبرد سایبری کنونی خواهد بود. سطوح بالایی از جرائم و جاسوسی سایبری وجود خواهد داشت ولی هیچ جنگ سایبری گسترده‌ای بین کشورها رخ نخواهد داد.

– **حوزهٔ نبرد:** فضای سایبری، درست مانند حوزه‌های هوا، زمین، فضا و دریا، مجموعهٔ گسترده‌ای از نبردهای انسانی را در بر خواهد گرفت.

– **تجزیه**: فضای سایبری به قلمروهای ملی تجزیه خواهد شد: نه یک اینترنت واحد بلکه مجموعه‌ای از اینترنت‌های ملی وجود خواهد داشت.

– **بهشت:** نوآوری‌های اجتماعی و فناورانه فضای سایبری را به محلی بسیار امن تبدیل خواهند کرد که وقوع جاسوسی، جنگ و جرم در آن بسیار دشوار است.

- **آخرالزمان سایبری:** فضای سایبری که همیشه بدون کنترل و غیرقابل‌کنترل است، به یک حوزهٔ آشفته با سطوح بالایی از فعالیت‌های هکری، تبهکارانه و تروریستی تبدیل خواهد شد. (ترادوک، ۲۰۱۶ :۸-۶)

۲-۷. مدل مفهومی تحقیق

در شکل سه مدل مفهومی تحقیق بیان‌شده است که به شرح زیر تشریح می‌گردد: عوامل محیطی مؤثر بر زیست‌بوم سایبری جمهوری اسلامی ایران عبارت‌اند از: دکترین امنیت ملی، تحولات ملی و بین‌المللی، توسعه فناوری، روندهای جهانی، آینده‌نگری، پیشران‌های فناوری.

ابعاد فضای سایبر ازنظر دفاعی امنیتی: عبارت‌اند از فیزیکی، اطلاعاتی و شناختی.

الف. در بعد فیزیکی محیط اطلاعات، زیرساخت‌های اتصال است که از انتقال، دریافت و ذخیره اطلاعات پشتیبانی می‌کند.

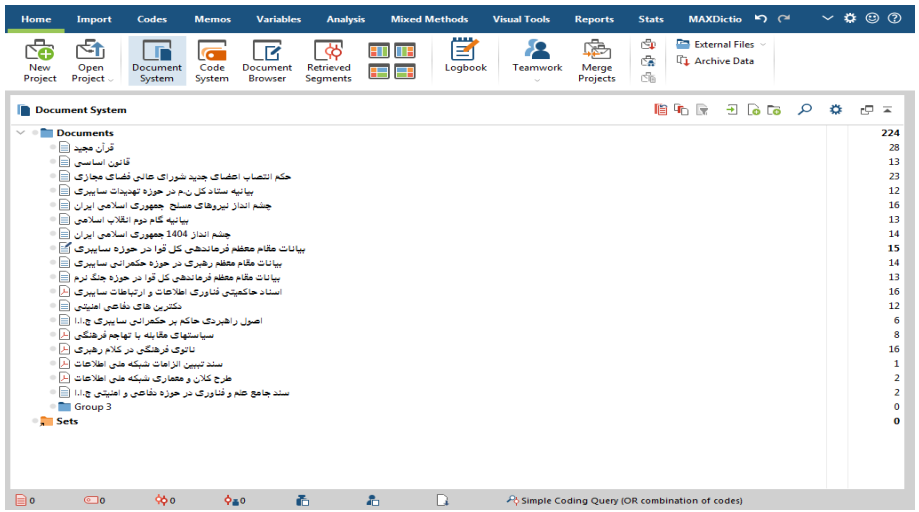
ب. درون بعد اطلاعاتی، محتوا یا داده است. ج-در بعد شناختی، ذهن کسانی که تحت تأثیر اطلاعات قرار می‌گیرند، وجود دارد.

مبانی احصاء دکترین فضای سایبر عبارت‌اند از اسناد بالادستی، فرامین رهبری، اندیشه‌های امامین انقلاب، مأموریت‌ها

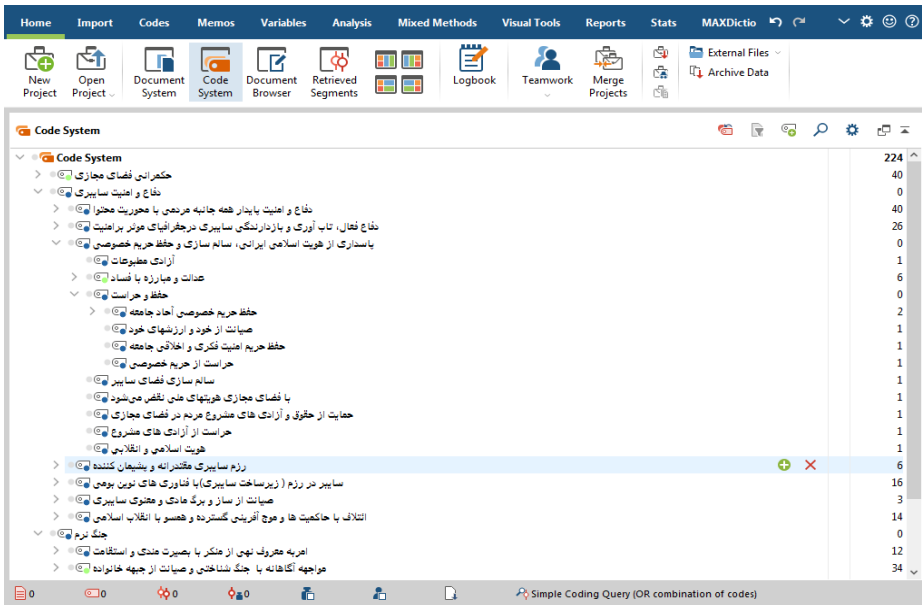
۳. یافته‌های تحقیق و تجزیه‌وتحلیل آن‌ها

برای به دست آوردن مضامین مرتبط با اصول دکترینی سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی، به تعدادی کلیدواژه مهم و مرتبط که بر مبنای آن‌ها مضامین از اسناد بالادستی جمهوری اسلامی ایران استخراج شود، نیاز بود. بر همین مبنا در ابتدا، ادبیات تحقیق به روش تحلیل مضمون، مورد واکاوی قرار گرفت. سپس با مراجعه به اسناد پایه بالادستی جمهوری اسلامی ایران اصول ثابت جمهوری اسلامی ایران موردبررسی قرار گرفت که مشخص گردید کلمات کلیدی ازجمله استقلال، آزادی، عدالت، مردم، بسیج، حکمرانی، کرامات و حقوق انسانی، انقلاب اسلامی، نفی سلطه گری و سلطه‌پذیری جهت

بررسی در اسناد می‌بایست مورد مداقه قرار گیرند. با دست آوردن این کلیدواژه‌ها و با استفاده از نرم‌افزار maxqda2020 و در سه مرحله کدگذاری (باز، محوری و انتخابی) ۲۲۴ کد از اسناد استخراج گردید. (شکل یک و دو)

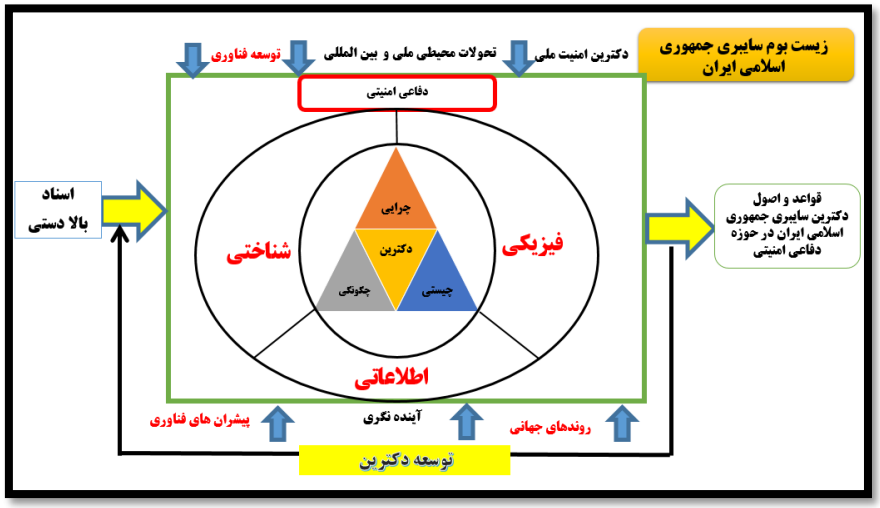


شکل ۱- استخراج ۲۲۴ کد از اسناد بالادستی در نرم افزار maxqda۲۰۲۰



شکل ۲- طبقه‌بندی کدهای تدوین‌شده

سپس کدهای به‌دست‌آمده به روش تحلیل مضمون به‌صورت مضامین پایه، مقوله و مفهوم دسته‌بندی گردید. در جدول زیر به‌صورت نمونه جدول یکی از مفاهیم به‌دست‌آمده، آورده شده است. در راستای اتقان کدهای بدست آمده، اسامی اسناد با استفاده از حروف اختصاری در کنارشان درج‌شده است که جدول کامل آن در پیوست یک آمده است.



شکل۳- مدل مفهومی تحقیق

جدول ۴- تدوین یک مفهوم از کدهای به‌دست‌آمده

شماره کد	نام سند	مضمون پایه (مقدمه)	مقوله	مفهوم
۳۴	KH	برابری و برادری همه انسان‌ها در کرامت انسانی	ارزش‌ها در نظام اسلامی	امربه معروف نهی از منکر با بصیرت مندی و استقامت
۱۴۲	GT	سبک زندگی		
۲۶۵	DD	تقویت ایمان، فرهنگ، معنویت، صلح، کرامت انسانی		
۶۸	CO	کرامت و ارزش والای انسانی		
۶۹	LT	رویکرد اخلاق‌مداری و عادلانه	رویکردهای نظام اسلامی	
۱۴۰	GT	معنویت و اخلاق		
۱۴۸	VN	توسعه کارآمد جامعه اخلاقی	اهمیت اخلاق در جامعه اسلامی	
۶۶	CO	ترویج دین و اخلاق		
۶۷	CO	رشد فضایل اخلاقی		
۶۴	CO	امربه‌معروف و نهی از منکر	مهم‌ترین عامل ارتقاء سطح جامعه	
۲۱۲	LS	نگاه خوش‌بینانه و امیدوارانه در جنگ نرم	رویکرد در جنگ نرم	
۲۱۸	LS	بصیرتی عمّارگونه و استقامتی مالک‌اشتروار در جنگ نرم	دیدگاه در جنگ نرم	

درنهایت؛ ۱۷ مفهوم استخراج گردید. لیکن آنچه در دکترین مهم است اصول موجز و تااندازه‌ای پایداری است که دامنه استفاده از آن را مبتنی بر قضاوت بهره‌بردار افزایش می‌دهد؛ بنابراین از ۱۷ مفهوم به‌دست‌آمده که در سه حوزه حکمرانی سایبری، دفاع و امنیت سایبری و جنگ نرم قابل‌طبقه‌بندی بودند، به سه اصل متناظر «استقلال سایبری از بیرون»، «اقتدار سایبری در درون» و «تواصی»[1] به‌عنوان اصول دکترینی رسیدیم.

۴. نتیجه‌گیری

۴-۱. جمع‌بندی

پس از انجام تجزیه‌وتحلیل بر روی کدهای به‌دست‌آمده، اصول دکترینی سایبری جمهوری اسلامی در قالب سه اصل (استقلال، اقتدار و تواصی) تدوین گردید. در بخش ادبیات نظری بیان شد که دکترین که دارای یک نقش هدایت‌کننده است درواقع از دوپایه نظری و عملی تشکیل گردیده است؛ بنابراین سه اصل به‌دست‌آمده از قسمت‌های نظری دکترین است و ۱۷ مفهوم به‌دست‌آمده به‌عنوان ملاحظات اساسی که رهنمودهای عملی راهبردی ارائه می‌دهند تعبیر می‌شوند که اصول و ملاحظات اساسی دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی در شکل سه آورده شده است.

---

۱. فرماندهی معظم کل قوا (مدظله العالی): برای مواجهه با دشمنِ فعال به دو عنصر مهم «بصیرت» و «صبر و استقامت» نیاز است. ایشان لازمه حفظ این دو خصوصیت مهم را، وجود «جریان تواصی» در جامعه برشمردند و گفتند: اگر زنجیره توصیه به صبر و حق در میان مردم برقرار باشد، احساس ناامیدی، تنهایی و ضعفِ اراده در جامعه به وجود نمی‌آید و جرأت اقدام نیز از بین نخواهد رفت. رهبر انقلاب اسلامی با تأکید بر اینکه یکی از اهداف اصلی دشمن در جنگ نرم، از بین بردن زنجیره تواصی است، خاطرنشان کردند: قطع جریان تواصی بسیار خطرناک است و جوانان به‌عنوان افسران جنگ نرم نباید بگذارند چنین اتفاقی بیفتد. ۱۳۹۹/۱۲/۲۹.

شکل ۲ –اصول و قواعد دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی

۴-۲. پیشنهادها

تلاش‌ها و موفقیت‌های جمهوری اسلامی ایران در حوزه دفاعی امنیتی در چهار دهه گذشته به اذعان کلیه کارشناسان داخلی و خارجی رسیده است. بخش دفاعی امنیتی فضای سایبر هم در زمره همین اقدامات قرار دارد. با توجه به‌ضرورت و اهمیت تدوین اسناد سایبری و به لحاظ تولید بازدارندگی این اسناد پیشنهادهایی به شرح زیر ارائه می‌شود:

پیشنهادهای تحقیقاتی

۱. دکترین سایبری دفاعی امنیتی جمهوری اسلامی ایران (در سطح راهبردی).
۲. دکترین سایبری سیاسی جمهوری اسلامی ایران.
۳. سیاست ها و راهبردهای سایبری دفاعی امنیتی جمهوری اسلامی ایران (منبعث از دکترین سایبری دفاعی امنیتی جمهوری اسلامی ایران)

۴. تاثیر دکترین سایبری دفاعی امنیتی جمهوری اسلامی ایران در ارتقاء توان رزم نیروهای مسلّح.

پیشنهادهایی اجرایی

۱. قواعد دکترینی بدست آمده در امور راهبردی سایبری دفاعی امنیتی پیاده‌سازی و بازخورد آن جهت توسعه دکترین سایبری استفاده شود.
۲. اسناد بالادستی سایبری در حوزه دفاعی- امنیتی، منبعث از دکترین سایبری تدوین گردد.
۳. نیروی انسانی توانمند و آموزش‌دیده در حوزه دکترین فضای سایبر، به آموزش و گفتمان سازی دکترین سایبری در حوزه دفاعی-امنیتی بپردازد.

*****

فهرست منابع

الف. منابع فارسی

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

۲. افشردی، محمدحسین؛ عراقی، عبدالله؛ زین‌الدینی، مجید (۱۳۹۶) ***اصول دکترین عملیاتی نزاجا و نزسا درنبرد ناهمطراز***، فصلنامه مطالعات دفاعی استراتژیک، سال پانزدهم، شماره ۷۰.

۳. ترابی، قاسم (۱۳۹۷)، ***چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر***، فصلنامه مطالعات راهبردی، شماره ۷۹، صفحات ۱۷۸-۱۷۳.

۴. ثروتی، محسن و همکار (۱۳۸۹) ***راهنمای تدوین دکترین در حوزه نظامی***، ناشر دبیرخانه هیئت عالی تجدیدنظر در آئین‌نامه‌های نیروهای مسلح ستاد کل نیروهای مسلح، تهران.

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

۶. خلیلی، رضا. (۱۳۸۶). ***دکترین، سیاست و استراتژی؛ نسبت سنجی نظری و مفهومی***. فصلنامه مطالعات راهبردی، سال دهم شماره ۳.

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

۸. دانشگاه جامع امام حسین علیه‌السلام، (۱۳۹۷)، ***تبیین قدرت سایبری***.

۹. ستاد کل نیروهای مسلّح ج.ا.ایران (۱۳۸۹) ***اصطلاحات و واژگان***.

۱۰. سید رحمانی (۱۳۹۳) ***مفهوم واژه دکترین***، سایت اندیشکده یقین

۱۱. شامحمدی، محمد؛ (۱۳۹۳). ***دکترین پدافند غیرعامل ج.ا.ا در برابر تهدیدات نامتقارن***، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاع ملّی.

۱۲. عباسی، محمد. بابایی، حسین و شاه‌محمدی، محمد. (۱۳۹۲). ***نهادینه شدن تهدیدات سایبری در ایالات‌متحده آمریکا***. امنیت پژوهی. دوره دوازدهم، شماره ۴۱، صفحات، ۱۹۳-۱۷۳

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

۱۴. غلامی، رضا (۱۳۹۸) ***الگوی شش‌ضلعی حکمرانی جمهوری اسلامی ایران در فضای مجازی***، مرکز ملّی فضای مجازی.

۱۵. کیانخواه، احسان؛ محمدی، علی (۱۳۹۷). ***واکاوی ماهیت سایبر***، مجموعه مقالات نخستین همایش ملّی دفاع سایبری.

۱۶. موسسه آموزشی و تحقیقات صنایع دفاعی (۱۳۸۶)، ***ارزیابی ابعاد گوناگون دکترین‌های امنیتی- دفاعی روسیه***، تهران.

۱۷. مرادی قاسم آبادی، فرج الله (۱۳۸۷)، ***مدیریت تحول و تعالی در سپاه***: انتشارات سمت.

۱۸. ولوی، محمدرضا، (۱۳۹۶)، ***دکترین سایبری جمهوری اسلامی ایران***، ستاد کل نیروهای مسلح.

۱۹. هلیلی، خداداد و همکاران (۱۳۹۷) ***مبانی تدوین دکترین قدرت سایبری ج.ا. ایران در سیاست‌های ابلاغی و اسناد بالادستی***، فصلنامه راهبرد دفاعی، سال شانزدهم، شماره ۶۳ پاییز ۱۳۹۷.

ب. منابع انگلیسی

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

۲. 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.

۳. Przygotowanie do druku, druk: Centrum Poligrafii Sp. z o.o. (2015).Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. Available at: www. jakubiccy.com.pl

٤. Reiss, megan (2017),*The US doesn't just need a cyber policy, it needs a cyber doctrine*,Available at: https://www.washingtonexaminer.com/the-us-doesnt-just-need-a-cyber-policy-it-needs-a-cyber-doctrin

٥. TRADOC G2 (2016). Mad Scientist the 2050 Cyber Army Technical Report.

پیوست یک: استفاده از علائم اختصاری برای اسناد استفاده‌شده

ردیف	سند	علامت اختصاری
۱	قرآن کریم	KH
۲	قانون اساسی جمهوری اسلامی ایران	CO
۳	حکم انتصاب اعضای جدید شورای عالی فضای مجازی	LT
۴	بیانیه ستاد کل ن.م در حوزه تهدیدات سایبری	AS
۵	چشم‌انداز نیروهای مسلح جمهوری اسلامی ایران	VA
۶	بیانیه گام دوم انقلاب	GT
۷	سند چشم‌انداز ۱۴۰۴ جمهوری اسلامی ایران	VN
۸	بیانات مقام معظم فرماندهی کل قوا در حوزه سایبری	LC
۹	بیانات مقام معظم رهبری در حوزه حکمرانی	LG
۱۰	بیانات مقام معظم فرماندهی کل قوا در حوزه جنگ نرم	LS
۱۱	اسناد حاکمیتی فناوری اطلاعات و ارتباطات سایبری	DI
۱۲	دکترین‌های دفاعی امنیتی	DD
۱۳	اصول راهبردی حاکم بر حکمرانی سایبری جمهوری اسلامی ایران	PG
۱۴	سیاست‌های مقابله با تهاجم فرهنگی	PC
۱۵	ناتوی فرهنگی در کلام رهبری	LN
۱۶	سند تبیین الزامات شبکه ملّی اطلاعات	DN
۱۷	طرح کلان و معماری شبکه ملّی اطلاعات	DA
۱۸	سند جامع علم و فناوری در حوزه دفاعی و امنیتی جمهوری اسلامی ایران	DS