فصلنامه امنیت ملی
سال نهم، شماره ۳۳، پاییز ۱۳۹۸
مقاله دهم از صفحه ۲٤۱ الی ۲۷۲

مقاله پژوهشی: متولیان تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری

علی ملائی [۱]، مهرداد کارگری [۲] و محمدحسین صنیعی [۳]

تاریخ دریافت: ۱۳۹۷/۷/۸ **تاریخ پذیرش: ۱۳۹۷/۹/۲۰**

چکیده

بازدارندگی یکی از مباحث اساسی در حوزه دفاعی- امنیتی هر کشور می‌باشد. از این رو تقویت و توسعه ادبیات راهبردی در حوزه بازدارندگی و به‌طور خاص در امنیت و دفاع سایبری به منظور بهره‌برداری سازمان‌های مسئول در راستای تدوین و اجرای سیاست‌های کلی فضای سایبر یکی از موضوعات پر اهمیت و اساسی می‌باشد. ایجاد قدرت بازدارندگی معتبر نقشی کلیدی در دفاع سایبری و تأمین امنیت دارا می‌باشد، برای رسیدن به این مهم می-بایست نهادهای خصوصی، عمومی و دولتی مورد نیاز در کنار یکدیگر و با هماهنگی، مأموریت‌های اصلی را انجام دهند. در این پژوهش قصد داریم تا با استفاده از روش مدل‌سازی ساختاری تفسیری متولیان مؤثر بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری را در نظام دفاع سایبری شناسایی نماییم و بررسی نماییم هر متولی در این فرآیند در چه سطحی، از کدام متولیان تأثیر می‌پذیرد و بر کدام متولیان تأثیر می‌گذارد.

در پایان نتایج تحقیق نشان می‌دهد که کلیه ۱٤ نهاد نظام دفاع سایبری بر روی فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری تأثیرگذار بوده و جهت حصول اهداف بازدارندگی مورد نیاز می‌باشند. در گام دوم با توجه به تأثیرگذاری نهادهای متولی بر روی یکدیگر، مبتنی بر ورودی و خروجی هر نهاد، سطح تأثیرگذاری هر نهاد تعیین شده است. نهادهای سطح بالاتر قدرت نفوذ بیشتری بر دیگر نهادها دارند و دارای قدرت تصمیم‌گیری بالاتری هستند و نهادهای سطوح پایین‌تر وابستگی بیشتری به دیگر نهادها دارند.

کلیدواژه‌ها: ایجاد قدرت بازدارندگی، تهدیدات و حملات سایبری، متولیان، فضای سایبر

۱. دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبر- (نویسنده مسئول) *a.mollaei@sndu.ac.ir*
۲. استادیار دانشگاه تربیت مدرس- *m_kargari@modares.ac.ir*
۳. استادیار دانشگاه عالی دفاع ملی- *saniee@sndu.ac.ir*

مقدمه:

بازدارندگی یکی از موضوعات اساسی در حوزه دفاعی- امنیتی هر کشور می‌باشد. از این رو تقویت و توسعه ادبیات راهبردی در حوزه بازدارندگی و به‌طور خاص در امنیت و دفاع سایبری به منظور بهره‌برداری سازمان‌های مسئول در حوزه سیاست‌های کلی فضای سایبر یکی از موضوعات پراهمیت و اساسی می‌باشد. کسب قدرت بازدارندگی یکی از عوامل مؤثر در دفاع سایبری می‌باشد، برای رسیدن به این مهم می‌بایست نهادها یا متولیان مورد نیاز با هماهنگی، مأموریت‌های اصلی را انجام دهند.

بازدارندگی یکی از موضوعات مهم و اساسی از منظر رهبری نظام جمهوری اسلامی ایران می-باشد، ایشان در بازدید سرزده از دانشگاه افسری امام علی (ع) بیان می‌دارند: ما امیدواریم با اراده و همت این جوانان برومند ارتش جمهوری اسلامی ایران به اوج قدرت بازدارندگی و اعتلای حقیقی در مأموریت شرافتمندانه دفاع از میهن، ملت، نظام اسلامی و اسلام عزیز دست یابد. در بیانی دیگر در مراسم سی‌امین سالگرد رحلت امام خمینی (ره) می‌فرمایند: هدف مقاومت عبارت است از رسیدن به نقطه بازدارندگی، هم در اقتصاد، هم در مسائل سیاسی کشور، هم در مسائل اجتماعی، هم در مسائل نظامی باید به نقطه‌ای برسیم که این نقطه بازدارنده باشد؛ یعنی بتواند جوری خود را نشان بدهد که دشمن را از تعرض به ملت ایران در همه زمینه‌ها منصرف کند، دشمن ببیند فایده‌ای ندارد و با ملت ایران نمی‌تواند کاری بکند. ما امروز در بخش نظامی تا حدود زیادی به این بازدارندگی رسیده‌ایم. این هم که می‌بینید روی مسئله موشک و مانند این حرف‌ها اصرار می‌کنند، به خاطر همین است، می‌دانند که ما به بازدارندگی رسیده‌ایم، به نقطه تثبیت رسیده‌ایم، می‌خواهند کشور را از این محروم کنند و البته هرگز نخواهند توانست.

بازدارندگی همچنین در اسناد بالادستی کشور یکی از موضوعات اساسی و مهم می‌باشد. در ابلاغ سیاست‌های کلی برنامه پنجم توسعه در چارچوب سند چشم انداز بیست ساله، ارتقاء توانمندی‌های دفاعی و قدرت بازدارندگی به منظور دفاع از حاکمیت تمامیت ارضی، منافع و امنیت ملی و مقابله مؤثر با تهدیدهای خارجی و ایجاد توازن منطقه‌ای با تأکید بر

۱ـ کسب دانش و فناوری‌های نو و نرم‌افزارهای پیشرفته دفاعی و نوسازی و بازسازی صنایع دفاعی، افزایش ضریب خودکفایی با توسعه تحقیقات و بهره‌مندی از همه ظرفیت‌های صنعتی کشور

۲ـ اهتمام به حضور نیروهای مردمی در امنیت و دفاع از کشور و انقلاب با تقویت کمی و کیفی بسیج مستضعفان

۳ـ گسترش پدافند غیرعامل

٤ـ امنیت پایدار مناطق مرزی و کنترل مؤثر مرزها، مورد تأکید قرار گرفته است. در حوزه فضای سایبر نیز در سند راهبردی پدافند غیرعامل کشور قدرت بازدارندگی مؤثر در برابر تهدیدات سایبری دشمن به عنوان اولین مؤلفه در ترسیم چشم‌انداز پدافند سایبری کشور مورد توجه قرار گرفته است.

پژوهش حاضر بخشی از مطالعه گروهی با عنوان «طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن» توسط گروه مطالعاتی متشکل از اساتید و دانشجویان دوره اول مدیریت راهبردی امنیت فضای سایبر در دانشگاه عالی دفاع ملی می‌باشد. این مطالعه گروهی توسط یک تیم اجرائی ۱۳ نفره با تقسیم کار مشخص در حوزه‌های مطالعاتی مورد نیاز انجام پذیرفته است. برای رسیدن به نظام دفاع سایبری در مطالعات گروهی انجام شده از چارچوب معماری زکمن استفاده شده است. شناخت نهادها و فرآیندهای مرتبط با نظام دفاع سایبری کشور یکی از اهداف مهم در مطالعه گروهی بوده است. در قالب یکی از خروجی‌های این مطالعه گروهی در چارچوب معماری سازمانی زکمن، تعداد ١٤ متولی برای نظام دفاع سایبری معرفی شده است. این متولیان در جدول شماره (۱) نمایش داده شده است. برای سطرهای چارچوب معماری زکمن از سطح راهبردی تا سطح فنی، در ستون‌ها در قالب سؤالات شش‌گانه چی، چرا، چگونه، کی (چه کسی)، کی (چه وقت) و کجا سلول‌هایی در نظر گرفته شده است که طراح می‌بایست برای رسیدن به جامعیت طرح خود هر یک از آن‌ها را در نظر بگیرد. کار بر روی هر یک از این سلول‌ها بسته به مسئله و نظام مورد نظر نیازمند انجام پژوهش‌های گوناگون است. پرشدن هر یک از این سلول‌ها در راستای یکپارچه بودن، از به وجود آمدن اعمال و اجزا تکراری جلوگیری می‌نماید. از منظر مدل‌های مرجع هرچند این چارچوب به‌طور خاص به مدل‌های خاصی اشاره نمی‌کند، اما استفاده از دیگر مدل‌های مرجع در دیگر استانداردها و چارچوب‌ها را نیز منع نمی‌کند. در این پژوهش مسئله اصلی بررسی تأثیرپذیری فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری از متولیان ١٤ گانه نظام دفاع سایبری می‌باشد. اینکه چه تعداد از این متولیان و در چه سطوحی بر فرآیند ایجاد بازدارندگی و پیشگیری از تهدیدات و حملات سایبری تأثیرگذار

هستند؟ تمرکز اصلی پژوهش را شکل خواهد داد. طراحی انجام‌شده در خصوص تعیین نهادهای تأثیرگذار بر فرآیند بازدارندگی، مستقل از وضع موجود و بدون هرگونه جهت‌گیری منبعث از آن و به عنوان یک طرح ایده‌آل ارائه گردیده است تا به یک چارچوب کلی برای شکل‌دهی نهادهای تأثیرگذار بر بازدارندگی در نظام دفاع سایبری دست یابیم. این چارچوب یک وضع مطلوب را ترسیم خواهد کرد تا در سطح کلان ملی برای ایجاد قدرت بازدارندگی نهادهای مورد نیاز ایجاد شوند.

جدول (۱): تعداد ١٤ نهاد تأثیرگذار بر نظام دفاع سایبری

عنوان	کد	عنوان	کد
متولی سیاست‌گذاری حوزه امنیت سایبر	N۱	متولی هماهنگی امنیت سایبری قوای سه‌گانه	N۸
متولی فرماندهی سایبری و تعیین وضعیت	N۲	متولی حفاظت از زیرساخت‌های ملی	N۹
متولی تدوین قوانین و مقررات سایبری	N۳	متولی نظارت و ارزیابی	N۱۰
متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N٤	متولی رصد، پایش تهدیدات و اشتراک‌گذاری	N۱۱
متولی امور بین‌الملل و دفاع سایبری کشورهای اسلامی	N٥	متولی تحقیقات، آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری	N۱۲
متولی مراکز عملیات امنیت شبکه و پاسخگویی	N٦	متولی رمز ملی و تصدیق هویت مجازی	N۱۳
متولی مقابله با جرائم سازمان‌یافته و تروریسم سایبری	N۷	متولی مدیریت محتوای سایبری و رسانه‌ها	N۱٤

اهمیت و ضرورت تحقیق: در این بخش در راستای تعیین اهمیت موضوع پژوهش با رویکرد ایجابی، به این می‌پردازیم که با انجام این مطالعه چه منافعی متوجه کشور می‌باشد، درحالی که ضرورت با رویکرد سلبی به این مسئله نگاه می‌کند که در صورت عدم توجه تبیین و شفاف‌سازی پاسخ به ابهامات مسئله تحقیق چه تهدیدات و چالش‌هایی برای کشور متصور است.

نظام مقدس جمهوری اسلامی ایران پس از پیروزی، در پی پیاده‌سازی اسلام ناب محمدی (ص)، به عناوین مختلف مورد هجمه‌های گوناگون قرار گرفته است. جنگ تحمیلی، تحریم‌های اقتصادی و توطئه‌های گوناگون دیگر را می‌توان نمونه بارز این تلاش‌ها برشمرد که در این مدت، مسیر انقلاب را دچار فراز و نشیب‌های زیادی نموده است. فناوری‌های فضای سایبر به‌طور گسترده و با سرعت بسیار زیادی در حال رشد هستند و به همین نسبت آسیب‌پذیری و تهدیدات خاص دیگری نیز متوجه ما خواهد بود. آنچه دستاوردها و نتایج مثبت این تحقیق بر آن تمرکز خواهد داشت، تشخیص متولیان تأثیرگذار بر فرآیند ایجاد بازدارندگی در فضای سایبر و سطح-

بندی آن‌ها می‌باشد. بسیاری جنگ سایبری را یکی از ارکان جنگ‌ها در امروز و آینده می‌دانند؛ بنابراین باید سازوکاری را برای مقابله با تهاجمات پیش‌رو دنبال کرد. از این‌رو یکی از نیازهای اساسی در سطح ملی تعیین چارچوب‌هایی برای ایجاد ساختارهای ملی، جهت ایجاد بازدارندگی در فضای سایبر است. با توجه به پیچیدگی‌های خاص فضای سایبر و وسعت حوزه دانشی آن هنوز بسیاری از متصدیان این حوزه در مدیریت این فضا دچار سردرگمی هستند. این امر نشان می‌دهد، به‌روزرسانی و بازطراحی ساختارهای موجود بازدارندگی سایبری، از اهمیت ویژه‌ای برخوردار است. این تحقیق از جنبه‌های مختلفی حائز اهمیت می‌باشد:

۱- تشخیص متولیان تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری،

۲- نگاه جدید کل‌نگرانه برای جامعه مخاطبان شامل سیاست‌گذاران، تصمیم‌سازان و تصمیم-گیران راهبردی در جهت ایجاد شفافیت و وضوح بیشتر،

۳- ایجاد نگاه سیستمی یا مدل محور در مقابل نگاه واکنشی در خصوص موضع بازدارندگی سایبری. در نگاه سیستمی مقابله با تهدید را قبل از وقوع آن، حین وقوع (حمله) و بعد از آن (بحران) به صورت برنامه‌ریزی شده در موقعیت زمانی و مکانی به صورت فعال دنبال خواهیم کرد ولی در نگاه واکنشی صرفاً وقتی عمل خواهیم کرد که اتفاقی افتاده باشد؛ بنابراین نظام دفاع سایبری می‌تواند ابزاری مفید، ضروری و حیاتی برای تصمیم‌گیران ارشد یک کشور باشد.

ضرورت تحقیق. سرمایه‌ها و دارایی‌های هر ملتی چه اقتصادی، چه فرهنگی، چه انسانی، صنعتی و نظامی همه شکل‌دهنده شاکله وجودی آن نظام هستند و پاسداری از آن‌ها یعنی پاسداری از یک ملت. فضای سایبر کشور بزرگ جمهوری اسلامی ایران نیز یکی از سرمایه‌ها و دارایی‌های مهم، استراتژیک و حیاتی این ملت غیور است که غفلت از پاسداری آن خسارات و صدمات سنگینی را برای نظام اسلامی به همراه خواهد داشت. ازاین‌رو محققین می‌بایست در راستای شکل‌دهی یک نظام دفاعی بروز، فعال، هوشمند، قدرتمند و آینده‌نگر تلاش نمایند تا تضمین‌های لازم برای دفاع مقتدرانه از فضای سایبری کشور تأمین گردد. به‌منظور مقابله با حملات سایبری، ساختارهای نظام‌مندی می‌بایست در کشورها ایجاد و عملیاتی گردد. جمهوری اسلامی ایران نیز از این قاعده مستثنا نبوده و حتی نسبت به دیگر کشورها در معرض خطر بیشتری قرار دارد و ناگزیر است که اقدامات جدی خود را در این خصوص انجام دهد و متناسب با شرایط نسبت به

بازطراحی ساختارهای موجود و شکل‌دهی ساختارهای جدید اقدام نماید. البته باید توجه داشت که برخی اقدامات در تدوین سندها و شکل‌دهی برخی نهادها در کشور انجام شده است که تا وضع مطلوب فاصله زیادی دارد، اما مستندات آن‌ها می‌تواند به‌عنوان اسناد بالادستی این تحقیق مورد استفاده قرار گیرد. نداشتن چنین پژوهش‌هایی در مدیریت دفاع سایبری باعث لطمات جبران‌ناپذیری به زیرساخت‌های حیاتی کشور شده و در شرایط بحران، انرژی کلانی برای هماهنگ‌سازی دستگاه‌های متولی صرف خواهد شد.

اهداف: در راستای رسیدن به نحوه فعل و انفعالات و تعامل داخلی فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری تمرکز اصلی این تحقیق بر سلول‌های سطر اول از نگاه راهبردی و به‌طور خاص به سلول‌های چه کسی، برای متولیان و چگونه برای فرآیندها در راستای احصاء و تعیین سطح نهادهای تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی می‌باشد؛ بنابراین اهداف اصلی تحقیق شناسایی متولیان و تعیین ارتباط و سطح تأثیرگذاری آن‌ها در فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری می‌باشد.

سؤالات تحقیق: متولیان و فرآیندهای بررسی شده در این تحقیق به لحاظ نظری، مجرد در نظر گرفته شده‌اند و در حالت کلی در تناظر یک نهاد فعال در شرایط کشور مدنظر محقق نبوده است. بلکه متولیان به صورت کلان و نظری، آنچه مورد نیاز یک نظام دفاع سایبری بوده است مورد توجه قرار گرفته است. در قالب سؤال تحقیق قصد داریم تا به پرسشی پاسخ گوییم که «از بین متولیان تأثیرگذار در نظام دفاع سایبری چه متولیانی بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری تأثیرگذار هستند؟» هر متولی در این فرآیند از چه متولیانی تأثیر می‌پذیرد و بر چه متولیانی تأثیر می‌گذارد؟ و این تأثیرگذاری و تأثیرپذیری در چه سطحی قرار دارد؟ بنابراین متولیان اصلی مؤثر بر فرآیند ایجاد قدرت بازدارندگی، متغیر وابسته تحقیق و زیرفرآیندها، مأموریت‌های مورد اشاره در اسناد بالادستی و مطالعات تطبیقی متغیرهای مستقل تحقیق را شکل خواهند داد.

مبانی نظری:

بازدارندگی سایبری: در کشور اسناد متنوعی از جمله ۱- سیاست‌های کلی برنامه ششم توسعه، ۲- سند چشم‌انداز جمهوری اسلامی ایران در افق ۱٤۰٤، ۳- ابلاغ سیاست‌های کلی نظام در امور

«امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)»، ٤- احکام انتصاب شورای عالی فضای مجازی، ٥- سیاست‌های کلی نظام در امور «پدافند غیرعامل» و ٦- سند راهبردی پدافند سایبری کشور، موضوع بازدارندگی را یکی از نیازهای اساسی تأمین امنیت کشور دانسته‌اند. «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی» مصوب ۱۵ آبان ماه ۱۳۹٦ در جلسه چهل و چهارم شورای عالی فضای مجازی، در این سند حوادث فضای مجازی دسته‌بندی شده و برای هر حادثه، نهاد مربوطه، نحوه هماهنگی، محوریت اجرا و مراحل همکاری تعیین شده است.

رهبر معظم انقلاب اسلامی در نامه‌ای به رئیس‌جمهور در تاریخ نهم تیرماه ۱۳۹٤، سیاست‌های کلی برنامه ششم توسعه که همزمان برای مجلس شورای اسلامی و مجمع تشخیص مصلحت نظام ارسال شده است را ابلاغ کردند. در بخش امور دفاعی و امنیتی، بند ۵۳ ارتقاء توان بازدارندگی کشور با توسعه توان موشکی و فناوری‌ها و ظرفیت تولید سلاح ها و تجهیزات عمده دفاعی برترساز با توان بازدارندگی و متناسب با انواع تهدیدات در نظر گرفته شده است (قوانین کشور, ۱۳۹٤).

در متن کامل سند چشم انداز بیست ساله جمهوری اسلامی ایران در افق ۱٤۰٤ هجری شمسی؛ که در تاریخ ۱۳ آبان ۱۳۸۲ توسط رهبری به سران قوای سه‌گانه ابلاغ شد، جامعه ایرانی در افق چشم‌انداز را با ویژگی‌هایی مشخص معرفی کرده است، جامعه‌ای، «امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه و پیوستگی مردم و حکومت» که بازدارندگی در آن مورد تأکید قرار گرفته است.

رهبری، سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)» را در تاریخ ۱۳۸۹/۱۱/۲۹ ابلاغ کردند. پیش‌نویس این سیاست‌ها در مجمع تشخیص مصلحت نظام به تدوین رسید. متن کامل این سیاست‌ها که با عنوان راهنمای دستگاه‌های اجرایی، تقنینی و نظارتی؛ خط‌مشی و جهت‌گیری نظام را در بخش مذکور تعیین می‌کند، در ۹ بند تنظیم شده است. بازدارندگی در مقابل هرگونه تهدید در بند پنجم «پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات» مورد تأکید قرار گرفته است.

رهبر انقلاب اسلامی سیاست‌های کلی نظام در امور «پدافند غیرعامل» را در تاریخ ۲۹ بهمن‌ماه ۱۳۸۹ ابلاغ کردند. متن کامل این سیاست‌های ابلاغی نیز که به عنوان راهنمای دستگاه‌های

اجرایی، تقنینی و نظارتی، خط‌مشی و جهت‌گیری نظام را در بخش مذکور تعیین می‌کند، در بند اول به شرح بازدارندگی با تأکید بر پدافند غیرعامل «که عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد» پرداخته شده است.

در سند راهبردی پدافند سایبری کشور متعلق به قرارگاه پدافند سایبری کشور «توسعه آمادگی دفاعی و بازدارندگی در مقابل تهدیدات و حملات سایبری» از موضوعات اساسی راهبردی پدافند سایبری کشور عنوان شده است (سازمان پدافندغیرعامل، ۱۳۹۳: ۸). در سند راهبردی پدافند سایبری کشور، در بند سوم این اصول در خصوص بازدارندگی این چنین آمده است: «دفاع به شیوه دشمن نتیجه‌ای برای ما در بر نخواهد داشت، فلذا باید از روش‌های بومی و خودی در دفاع بهره جست. همچنین دفاع باید تمام جوانب مربوط به فضای به هم پیوسته و شبکه‌ای شده سایبری را در برگیرد به گونه‌ای که هیچ حلقه ضعیفی در زنجیره سرمایه‌های کشور وجود نداشته باشد. چنین دفاعی دشمن را با در بسته مواجه نموده و انگیزه‌های وی را برای تهدید و حمله کاهش خواهد داد و در صورت اقدام هزینه‌های سنگینی را برای وی تحمیل خواهد کرد» (همان: ۹).

در بخش اهداف کلان در افق چشم‌انداز قرارگاه پدافند سایبری کشور آمده است، در بند دوم، دوازدهم و بیستم به بازدارندگی اشاره شده است. این اهداف به ترتیب عبارتند از «ارتقای آمادگی دفاعی و بازدارندگی کشور در مقابل تهدیدات و حملات سایبری کشورهای متخاصم»، «سازماندهی، آموزش، هدایت، کنترل و ارزیابی مداوم دستگاه‌های کشور در راستای ارتقاء کارایی دفاعی و نیل به بازدارندگی پدافندی از طریق فعال‌سازی پدافند سایبری» و «طبقه‌بندی و سطح-بندی سایبری زیرساخت‌ها، آسیب‌شناسی در برابر تهدیدات، ایمن‌سازی، پایدارسازی و مصونیت بخشی به زیرساخت‌های سایبری کشور و ارتقای بازدارندگی آن‌ها» (همان).

بازدارندگی در تعریف پدافند سایبری این‌گونه اشاره شده است: «پدافند سایبری: بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیر سایبری کشور، به منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه-های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به نحوی که

امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید» (همان: ٦). در بیانیه مأموریت این سند افزایش توان بازدارندگی و ارتقاء پایداری به منظور مأیوس سازی دشمنان از حمله به سرمایه‌ها و منافع ملی از مأموریت‌های این قرارگاه عنوان شده است (همان: ۱۲).

در راهبردهای پدافند سایبری کشور در بند شانزده این‌گونه اشاره شده است: «کاهش آسیب-پذیری، پایدارسازی، مصون‌سازی، ارتقاء توان بازدارندگی زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری» و بازدارندگی مورد تأکید قرار گرفته است (همان: ۲۱).

با توجه به این اسناد قوای سه‌گانه کشور، شورای عالی فضای مجازی و نیروهای مسلح و نظامی در سطح کلان ملی مورد توجه قرار گرفته است. در پایان این بخش در می‌توان عنوان کرد بازدارندگی در فضای سایبر یک موضوع مهم در اسناد راهبردی کشور می‌باشد و به‌طور صریح مورد اشاره قرار گرفته است و نیز بر اهمیت و ضرورت آن تأکید شده است. در نهایت بازدارندگی مجموعه‌ای از توانمندی‌ها، متناسب با انواع تهدیدات و آسیب‌پذیری‌ها به صورت همه‌جانبه می-باشد به‌گونه‌ای که دشمنان را از حمله به سرمایه‌ها و منافع ملی منصرف سازد و در نتیجه آن موجبات ارتقاء و تداوم پایداری فراهم گردد.

تهدیدات و حملات: برخی از دلایل برای تهدیدگران شخصی و سازمان‌های خارجی در جهت تلاش برای بهره‌برداری از یک آسیب‌پذیری در خدمات و سامانه‌های اطلاعاتی می‌تواند شامل مواردی چون: ۱- کم کردن تلاش‌ها برای کامل شدن یک فرآیند، ۲- سود مالی، ۳- انتقام، ٤- کسب دانش یا اطلاعات، ٥- نمایش قدرت، ٦- به دست آوردن شناخت و احترام رقیب، ۷- ارضای کنجکاوی، ۸- پیشبرد اهداف سیاسی و اجتماعی و ۹- ترساندن برخی اهداف یا گروه‌های خاص باشد. انگیزه‌های سازمان‌های خارجی برای تهدید می‌تواند شامل مواردی چون ۱- به دست آوردن مزیت رقابتی، ۲- به دست آوردن مزیت‌های اقتصادی، ۳- به دست آوردن مزیت‌های نظامی، ۳- به دست آوردن مزیت‌های سیاسی، ٤- پیشبرد اهداف سیاسی و اجتماعی، ٥- سود مالی، ٦- ترساندن برخی اهداف یا گروه‌های خاص باشد (***DIA_New_Zealand,*** ۲۰۱٤: ۱٦).

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق

دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ایجاد اختلال در ارائه خدمت تهدید راهبردی سایبری گفته می‌شود (سازمان پدافندغیرعامل، ۱۳۹۳: ٤).

فناوری‌هایی که برای هدایت و ایجاد به ما قدرت می‌دهد همان فناوری‌ها می‌تواند اختلال و تخریب ایجاد نماید. تهدیدات سایبری، به امنیت ملی آمریکا، حتی می‌تواند فراتر از اهداف نظامی باشد؛ این تهدیدات می‌تواند همه‌ی جنبه‌های جامعه را تحت تأثیر قرار دهد؛ و هکرها و دولت‌های خارجی با اجرای نفوذهای پیچیده به شبکه‌ها و سامانه‌های اساسی زیرساخت شهری، توانمندی‌هایشان را افزایش می‌دهند. دولت‌های خارجی، گروه‌های تروریستی، عناصر مجرم و همکاران بی‌تعهد از جمله افرادی هستند که می‌توانند تهدید آفرینی نمایند (***DOD_OF_USA,*** ۲۰۱۱: ٤).

دشمنان به‌طور قابل توجهی در فضای سایبر سرمایه‌گذاری کرده‌اند، زیرا ظرفیت‌های انکاری قابل قبولی را به آن‌ها خواهد داد تا کشور ما را مورد هدف قرار دهند و به منافع ما خسارت وارد نمایند. علاوه بر دولت‌ها بازیگران غیردولتی مانند گروه‌های تروریستی از فضای سایبر در راستای جذب مبارزان، تبلیغات و به دست آوردن اقدامات تخریب‌کننده استفاده می‌کنند. مجرمان نیز به‌طور خاص برای مؤسسات مالی تهدید جدی در فضای سایبر به شمار می‌آیند و گروه‌های ایدئولوژیک اغلب از هکرها برای پیشبرد اهداف سیاسی‌شان استفاده می‌کنند. تهدیدات دولتی و غیردولتی در برخی مواقع با یکدیگر ترکیب می‌شوند، نهادهای میهن‌پرست به عنوان ناجی برای دولت‌ها عمل می‌کنند و غیردولتی‌ها می‌توانند زمینه را برای عاملین مستقر در دولت فراهم کنند، این شرایط اسناددهی[۱] را با مشکل مواجه می‌سازد و احتمال اشتباه محاسباتی را بالا می‌برد (***DOD_OF_USA,*** ۲۰۱۵: ۹).

در این سند کشورهای روسیه و چین به عنوان کشورهای درجه اول تهدیدکننده فضای سایبر آمریکا معرفی شده‌اند و بعد کشورهای ایران و کره‌شمالی در درجه دوم اشاره شده‌اند. رقبای راهبردی ایالات‌متحده آمریکا، در حال به‌کارگیری کارزارهایی برای از بین بردن مزایای نظامی، تهدید زیرساخت‌ها و کاهش موفقیت‌های اقتصادی ما هستند. وزارت دفاع باید به‌وسیله افشاء، مختل کردن و تحقیر[۲] این فعالیت‌ها که منافع ایالات‌متحده را تهدید می‌کند به این فعالیت‌ها پاسخ

۱-Attribution

۲-Degrading

دهد و امنیت سایبری و تاب‌آوری اهداف بالقوه کلیدی و همکاری نزدیک با دیگر متولیان و وزارتخانه‌ها و نیز شرکا و متحدانمان را تقویت نماید (***DOD_OF_USA,*** ۲۰۱۸: ۲).

تهدیدات راهبردی سطحی از تهدید هستند که در آن وقوع تهدیدات و حملات خسارات جبران‌ناپذیری را برای کشور به وجود می‌آورد و برای مهار آن‌ها در سطح شوراهای ملی تصمیم-گیری می‌شود. تهدیدات سایبری راهبردی تهدید به آرمان‌ها، راهبردهای ملی، اهداف کلان نظام، منافع، دارایی‌ها و سرمایه‌های ملی در فضای سایبر می‌باشد (ملائی، ۱۳۹۲: ۸۰). جامعه دیجیتالی فرانسه در حال شتاب گرفتن می‌باشد، بی‌وقفه خدمات، محصولات و مشاغل دیجیتال رشد می‌کند. این موضوع به یک مسئله ملی تبدیل شده است. گذار دیجیتال به نفع نوآوری و رشد است، اما با این حال هم‌زمان مخاطراتی را برای دولت، ذینفعان اقتصادی و شهروندان دارد. جرائم سایبری[۱]، جاسوسی[۲]، تبلیغات[۳]، خرابکاری[۴]، بهره‌برداری بیش از حد یا استثمار داده‌های شخصی[۵] اعتماد و امنیت دیجیتال ما را تهدید می‌کنند (***Prime_Minister_of_France,*** ۲۰۱۵: ۲).

نیت‌ها (پول، دانش، قدرت، مزیت‌های عملیاتی و ...) هنوز باقی مانده است، اما امکانات به سرعت رشد یافته است، با وسایلی بسیار محدود، انقلاب اینترنتی جاسوسی، خرابکاری، تروریسم، براندازی[۶]، جرائم، فرماندهی و کنترل، تبلیغات و عملیات نظامی- سایبری را آسان ساخته است. در فضای سایبر حمله به نسبت دفاع ساده‌تر، ارزان‌تر و سریع‌تر صورت می‌گیرد (***DOD_of_Belgian,*** ۲۰۱٤: ۵). در سند (***MOD_UK,*** ۲۰۱۱: ۱۵) مواردی چون جرائم، جاسوسی، تروریست‌ها، هکتیویست‌ها به عنوان تهدیداتی که منافع بریتانیا را در فضای سایبر تحت تأثیر قرار می‌دهند، معرفی شده‌اند.

انگیزه‌های عامل تهدید، می‌تواند توسط فاکتورهایی همچون قابلیت‌ها و فرصت‌ها تسریع یا تعدیل شود. به عنوان مثال تجهیزات، سطح خبرگی و تجربه تهدیدکننده روی آن تأثیرگذار است همچنین وجود فرصت‌هایی برای اعمال تهدید که به‌طور خاص می‌توان به آسیب‌پذیر بودن هدف

۱-Cybercrime

۲-Espionage

۳-Propaganda

۴-Sabotage

۵-Excessive exploitation of personal data

۶-Subversion

اشاره کرد. همچنین می‌بایست با توجه به هر بافت[۱] یا بستر کسب‌وکار خاص سازمان‌ها و دولت‌ها این انگیزه‌ها شناسایی شود. به نظر می‌رسد با توجه به بافت حیات ملت‌ها یا کشورها و تعاملات بین‌الملل در شناسایی انگیزه‌های تهدیدکننده می‌بایست مؤلفه‌های نیازهای حیاتی ملت‌ها، منفعت‌طلبی‌ها و قدرت کشور در حوزه سایبری توجه نمود. این منفعت‌ها می‌تواند بر اساس منافع اقتصادی، سیاسی، اجتماعی و ... شکل بگیرد. شاید نتوان فهرست یکسان و طبقه‌بندی ثابتی از انگیزه‌ها، تهدیدات و حملات سایبری فراهم نمود، اما بسته به شرایط کشور رسیدن به یک طبقه-بندی قرار دادی و مورد توافق متولیان مرتبط برای رسیدن به بازدارندگی ضروری می‌باشد. تهدیدات به صورت بالقوه، پتانسیلی را برای وقوع حملات فراهم می‌سازند و حملات نمودی بالفعل از تهدیدات می‌باشند. وجوه اشتراک توانمندی بهره‌برداری از آسیب‌پذیری در دارایی‌ها و سرمایه‌های مادی و معنوی ملی، با انگیزه‌هایی چون شهرت، منافع مالی، سیاسی، اجتماعی، تلافی، کسب مزیت‌های رقابتی، پتانسیلی را برای بازیگران در جهت وارد نمودن ضربه به دارایی و سرمایه‌ها فراهم می‌سازد که شکل‌دهنده تهدیدات می‌باشند و عملی شدن این تهدیدات حملات سایبری را به وجود خواهند آورد.

نظام دفاع سایبری: به‌کارگیری اقدامات حفاظتی مؤثر برای به دست آوردن یک سطح مناسب از امنیت سایبری برای کاهش مخاطره امنیتی به یک سطح قابل‌پذیرش، عملیات دفاعی و در نتیجه آن تضمین عملکرد حاصل می‌شود. دفاع سایبری از وظائف و تکالیف، حفاظت[۲]، کشف[۳]، پاسخ[۴] و بازیابی[۵] تشکیل شده است (***DOD_of_Belgian,*** ۲۰۱٤: ۱۸).

اصطلاح دفاع سایبری به همه اقدامات برای دفاع از فضای سایبر به‌وسیله نیروهای نظامی و ابزارهای مناسب برای احصاء اهداف راهبردی- نظامی اشاره می‌کند. دفاع سایبری یک سامانه یکپارچه شامل پیاده‌سازی همه اقدامات مرتبط به فناوری اطلاعات و ارتباطات و امنیت اطلاعات، قابلیت‌های تیم نظامی آمادگی واکنش سریع به حملات و تهدیدات[۶] و عملیات شبکه‌ای رایانه‌ای[۷]

۱-Context
۲- Protect
۳- Detect
۴- Respond
۵- Recover
۶- Computer emergency Readiness Team
۷- Computer Network Operation

همچنین پشتیبانی از قابلیت‌های فیزیکی ارتش می‌شود (***FCR_Austria,*** ۲۰۱۳: ۲۱). در پایگاه اطلاع‌رسانی قرارگاه پدافند سایبری کشور (پاپسا[۱]) جهت معرفی قرارگاه پدافند سایبری کشور این‌گونه آمده است: در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز به این فضا منتقل و یا اساساً در این فضا شکل گرفته است. عمده فعالیت‌های رسانه‌ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب‌وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیری یافته و از میان شاخص‌های تعیین‌شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تأثیر عمده می‌پذیرد. به عبارت دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی با این فضا درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را به مخاطره خواهد انداخت. ضرورت و اهمیت صیانت از فضای سایبری کشور در مقابل انواع تهدیدات و تهاجمات سایبری و به‌ویژه جنگ سایبری، موجب گردید قرارگاه پدافند سایبری کشور با هدف تمرکز بر دفاع از زیرساخت‌های حیاتی، حساس و مهم کشور در مقابل انواع تهدیدات و تهاجمات سایبری ایجاد شود. قرارگاه پدافند سایبری کشور وظیفه صیانت از مرزهای سایبری کشور در حوزه غیرنظامی و به‌ویژه در حوزه ایمن‌سازی زیرساخت‌های حیاتی و حساس واقع شده در این فضای سایبری را بر عهده خواهد داشت. این نکته حائز اهمیت است که پدافند سایبری بخشی از مقوله دفاع سایبری است و دفاع سایبری دارایی مؤلفه دیگری چون آفند سایبری نیز می‌باشد.

۱- https://goo.gl/kVSMN۸

آفند و پدافند دو مؤلفه اصلی در دفاع می‌باشند. مجموعه اقدامات بازدارنده، رفع‌کننده، دفع‌کننده و بازیابی‌کننده که به‌منظور پیش‌گیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد (مطالعه گروهی طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، ۱۳۹۵). در نهایت می‌توان گفت در امنیت به دنبال وضعیتی هستیم که مخاطرات اساسی به سطحی که قابل‌پذیرش باشد کاهش یابد. تأمین امنیت یکی از اهداف دفاع می‌باشد. امنیت و دفاع به لحاظ محدوده کاربرد آن می‌تواند فردی، گروهی، سازمانی و ملی باشند. حوزه دفاعی در کلان ملی مجری کنترل‌های امنیتی و تأمین‌کننده امنیت در ارزش‌ها، زیرساخت‌ها، سرمایه‌های ملی می‌باشد. هرچند در کشور بخش‌هایی مانند پلیس در تأمین امنیت اقدام می‌کنند، اما آنچه حوزه دفاعی را متمایز می‌سازد؛ عملکرد آن در دفاع از ارزش‌های ملی و حاکمیت ملی یا امنیت ملی در مقابل حملات و تهدیدات خارجی می‌باشد.

اگر از منظر طراحی بخواهیم نظام دفاع سایبری را مبتنی بر معماری زکمن توصیف نمائیم، می‌توان گفت در صورتی یک نظام دفاع سایبری جامع و کامل شکل خواهد گرفت که در معماری آن، کلیه سلول‌های آن در ماتریس زکمن از سطح راهبردی تا فنی به پرسش‌های شش‌گانه پاسخ داده شده باشد. نظام دفاع سایبری مجموعه‌ای از متولیان، ساختارها، فرآیندها، سامانه‌ها، منابع مادی، اعتباری و سرمایه‌های انسانی با اهدافی مشخص است که مأموریت آن حفاظت از ارزش‌ها، دارایی‌ها و سرمایه‌ها، بازداری، دفع و رفع تهدیدات و حملات در فضای سایبر در سطوح راهبردی، عملیاتی، تاکتیکی و تکنیکی می‌باشد.

پیشگیری و بازدارندگی از حملات سایبری: بازدارندگی به زبان ساده متقاعد ساختن یک حریف است به‌طوری که او بداند هزینه‌های مخاطره اجرای اقدامات خصمانه خیلی بیشتر از مزایای حاصل از آن است ***(Payappalli, Zhuang, & Jose,*** ۲۰۱۷:۱). در مقاله ***(Mowbray,*** ۲۰۱۰) قابلیت‌های بازدارندگی در سطح راهبردی و فنی مورد توجه قرار گرفته است. برخی معماری‌های راهکار پیشنهاد شده و سرانجام نتیجه تحقیق در قالب یک معماری مفهومی برای بازدارندگی سایبری ارائه شده است. در تحقیق ***(Beidleman,*** ۲۰۰۹: ۱٦) پتانسیل حملات سایبری را که به شدت خسارات سنگینی به امنیت ملی کشور وارد می‌کند مورد کاوش قرار می‌دهد و حملات سایبری را به عنوان یک عمل جنگی تعیین می‌کند. همچنین در روشی توصیفی و تحلیلی ارائه شده است که حملات سایبری در شرایطی خاص می‌توانند به عنوان عملی در جنگ به‌کار گرفته شوند. تعریف هنجارهای بین‌المللی در فضای سایبر به بازدارندگی می‌تواند کمک کند.

بازدارندگی برای دلسرد کردن تجاوزگر به‌کار می‌رود و بازدارندگی پیشنهادهایی را برای محافظت از منافع ملی ارائه می‌کند. این تحقیق تلاش می‌کند تا هنجارهای موجود بین‌المللی را برای فضای سایبر به‌کار گیرد و همچنین چگونگی به‌کارگیری مفاهیم سنتی بازدارندگی را در فضای سایبر مورد بررسی قرار می‌دهد. بازدارندگی پیشنهادهایی را برای محافظت از منافع ملی آمریکا مطرح می‌نماید. به‌طورکلی بازدارندگی یک حالت ذهنی است، به‌نوعی مفهومی است، از نفوذ بر دیگر کشورها، برای عدم اجرای گزینه‌هایی که برخلاف منافع کشور مورد نفوذ می‌باشد. در مقاله ***(Moore,*** ۲۰۰۸) به صورت تحلیلی و توصیفی اساس بازدارندگی راهبردی (بازدارندگی مرسوم، بازدارندگی هسته‌ای و بازدارندگی درخور یا مناسب) مورد بررسی قرار گرفته است. تهدیدهای رو به رشد در فضای سایبر بررسی شده‌اند و خصوصیات بازدارندگی سایبری نیز تعیین شده‌اند و بازدارندگی انکار، بازدارندگی تنبیه، تکنیک‌ها و تعیین حد آستانه و توسعه سیاست‌های ملی مورد تحلیل و بررسی قرار گرفته است. در تحقیق ***(Hausken & Zhuang,*** ۲۰۱۲) مدافع برای بازداری مهاجم از حملات تروریستی تکرارشونده، یک دارایی را تحت کنترل خود قرار می‌دهد و تأثیرات پویائی و نیز اجزا اساسی بازی‌های ضدتروریستی، شامل هزینه‌های دفاعی، هزینه‌های حمله و ارزشیابی سرمایه را مورد مطالعه قرار می‌دهد.

نظریه بازدارندگی بعضی از اقدامات متقابل و محرک‌ها را برای پیشگیری پیشنهاد می‌کند. بازدارندگی سایبری می‌تواند به عنوان توانمندی سازمان‌ها و مؤسسات برای انکار، محافظت و اقدام متقابل علیه حملات سایبری تعریف شود ***(Liles & Davidson,*** ۲۰۱۳:٤). بازدارندگی سایبری گزینه‌های بیشتر و قابل انعطاف‌تری به نسبت روش‌های توسعه‌یافته در عصر هسته‌ای جنگ سرد در اختیار می‌گذارد. حتی بیش از اقدام تلافی‌جویانه سنتی، بازدارندگی سایبری گزینه‌هایی همچون اتخاذ اقدام قانونی، ایجاد پوشش در شبکه، مقاوم‌سازی و وابستگی متقابل را شامل می‌شود و همچنین راه‌های جدیدی را برای به‌کارگیری متدولوژی‌های پذیرفته‌شده مانند عدم آسیب‌پذیری را ارائه می‌کند***(Jensen,*** ۲۰۱۲: ۷۷۳).

هدف بازدارندگی جلوگیری از اقدامات خصمانه به‌وسیله تضمین این امر در ذهن یک متخاصم است که تفهیم کند مخاطره عملش از مزایای آن بیشتر است، به‌طوری که متخاصم عدم اقدام را ترجیح دهد ***(Jensen,*** ۲۰۱۲: ۷۷۹). بازدارندگی اساساً روی تهدید یک مهاجم بالقوه با پاسخ تنبیهی به منظور بازداری از وقوع حمله تمرکز دارد. هرچند به دلیل ویژگی‌های خاص

فضای سایبر، یک سیاست بازدارندگی کلی مبتنی بر تهدید اقدام تلافی‌جویانه، ممکن است برای بازدارندگی مناسب نباشد و در برخی شرایط ممکن است غیرسازنده[۱] باشد؛ بنابراین چهار عامل اساسی شامل: ۱- جریمه (ایده آشنایی که هزینه‌های حمله را از طریق تنبیه افزایش می‌دهد) ۲- خنثی‌سازی (ایده‌ای که از طریق مقاوم‌سازی و یا قابلیت‌های بازیابی، حملات را بی‌فایده و خنثی می‌سازد) ۳- وابستگی (ایده‌ای از وابستگی داخلی به‌طوری که نفوذ را تعدیل و مدیریت می‌کند) و ٤- عدم سازندگی (ایده‌ای که یک عکس‌العمل تضمین‌شده می‌تواند از رفتار خصمانه ممانعت نماید) در راستای تأمین بازدارندگی وجود دارد***(Taipale,*** ۲۰۱۰ :۲***)***. جنبه‌های مختلفی از بازدارندگی وجود دارد، اما بازدارندگی عموماً به‌وسیله تهدید از دو عنصر ۱-تنبیه مهاجم به‌وسیله تحمیل کردن هزینه‌های غیرقابل‌پذیرش و ۲- جلوگیری از مهاجم از موفقیت در حمله‌اش صورت می‌پذیرد***(Kesan & Hayes,*** ۲۰۱۱:٤۳٤***)***. بازدارندگی سایبری همانند دیگر بازدارندگی‌ها وقتی موفق خواهد شد که دشمن تصمیم به اقدام خصمانه نمی‌گیرد. این تصمیم از دو ارزیابی جداگانه پیروی می‌کند، اول هزینه‌های تخاصم بیشتر از مزایای آن باشد و دوم مزایای خودداری در فضای سایبر بیشتر از هزینه‌ها باشد ***(Goodman,*** ۲۰۱۰:۱۰۷***)***.

بازدارنده در صورتی موفق خواهد شد که تهدید در سطحی باشد که هزینه‌های دشمن در صورت اجرائی کردن عمل خصمانه بیشتر از مزایای آن باشد***(Moore,*** ۲۰۰۸:۱٤***)***. در مقاله ***(Beidleman,*** ۲۰۰۹:۱٦***)*** ایده اصلی بازدارندگی از نگاه وزارت دفاع «نفوذ قاطعانه بر محاسبات تصمیم‌گیری متخاصم به منظور جلوگیری از عمل خصومت‌آمیز علیه منافع حیاتی ایالات‌متحده» گفته شده است. کشور بازدارنده تصمیم می‌گیرد تا اقدامی انجام نشود، زیرا آن‌ها فهمیده‌اند یا درک کرده‌اند که انجام چنین عملی پیامدهای غیرقابل تحملی را به همراه خواهد داشت. ایده تأثیر بر تصمیمات کشورها فرض می‌کند که کشورها بازیگران عاقلی هستند، مایل‌اند تا هزینه‌های درک شده از یک عمل علیه منافع درک شده را اندازه‌گیری کنند و یک برنامه عمل انتخاب کنند به صورتی که این برنامه منطقاً مبتنی بر نرخ هزینه و فایده‌ی قابل استدلال می‌باشد.

بازدارندگی یک رابطه روان‌شناختی می‌باشد، هدف آن شکل‌دهی به ادراک‌های حریف، انتظارات و در نهایت تصمیمات آن درباره شروع حمله می‌باشد؛ بنابراین بازدارندگی، یک حریف نیاز دارد، کسی که در حال فکر کردن است یا تصور می‌کند به راحتی می‌تواند حمله کند

۱-Counter productive

(Morgan, ۲۰۱۰:۵٦***)***. الزامات کلیدی و اساسی برای حصول قابلیت‌های مؤثر برای ایجاد راهبرد بازدارندگی مؤثر آمریکا از دیدگاه نویسندگان (***Kugler,*** ۲۰۰۹:۱۸) شامل موارد زیر می‌شود: ۱- یک سیاست تدوین‌شده رسمی، محکم و شفاف مقاصد ما را برای بازداری حملات سایبری مشخص خواهد کرد، ۲- یک سامانه آگاهی موقعیتی کلان سراسری که طیف کاملی از تهدیدات سایبری و شرایطی که این تهدیدات به وجود می‌آیند را رصد کند، ۳- سیستم فرماندهی و کنترلی که مجوزهای لازم را برای پاسخ‌های چند منطقه‌ای و وطنی به تهدیدات سایبری فراهم سازد، ٤- دفاع سایبری مؤثر که نیروهای نظامی و وطن آمریکا را به همراه اولویت‌هایی برای دفاع از زیرساخت‌های اساسی فراهم می‌سازد، ۵- طیف وسیعی از قابلیت‌های آفندی متقابل شامل حملات و دیگر ابزارها برای اثبات قدرت ایالات‌متحده به منظور تضمین بازدارندگی قبل، حین و بعد از بحران‌ها، ٦- هماهنگی یکپارچه بین سازمان‌های داخلی و همکاری با متحدان و شرکا در اروپا، آسیا و دیگر قاره‌ها که به خوبی توسعه‌یافته باشد و ۷- روش‌های بازدارندگی سایبری، معیارها و تجاربی که می‌تواند به فرآیند برنامه‌ریزی کمک کند.

در مقاله (دولت‌آبادی, ۱۳۹۲: ۸۰) مؤلفه‌های بازدارندگی راهبرد نظامی ایران را برشمرده است. این راهبرد که متکی بر عنصر دفاعی و مشخصاتی همچون توان بازدارندگی موشکی، تهدید امنیت صدور انرژی، دفاع مسطح (موزاییکی)، بهره‌گیری از کمک متحدان راهبردی، جنگ نامتقارن و عملیات استشهادی می‌باشد، تاکنون در بازداشتن دشمنان از هرگونه اقدام تحریک‌آمیز مؤثر بوده است. نکته مهم در خصوص راهبرد نظامی ایران که آن را از بسیاری دیگر از کشورها متمایز می‌سازد، مبتنی بودن این راهبرد بر دفاع به‌جای حمله می‌باشد. در حقیقت بازدارندگی مورد تأکید ایران بازدارندگی از نوع دفاعی بوده که حفاظت از تمامیت ارضی، منافع ملی و ساختار قانون اساسی کشور را به جای تعدی به خاک دیگر کشورها هدف اساسی خود قرار داده است. در مقاله (وحیدپور، ۱۳۹۲) نویسنده اشاره دارد که آگاهی می‌تواند عاملی جلوگیری کننده از تهدید باشد. همچنین مؤلفه‌هایی چون وجود تسلیحات آفندی باعث اعتباربخشی خواهد شد و نیاز به پیمان‌های بین‌المللی در حوزه سایبر و حضور غیرنظامیان در خط مقدم جنگ سایبری بر موفقیت بازدارندگی تأثیرگذار است. نویسنده در پایان می‌نویسد: به بیانی دیگر در دنیای دیجیتالی شده کنونی ملتی قادر خواهد بود پیروز کارزار باشد که بتواند توانمندی-

های بالقوه خود را در جهت صحیح و با سیاستی زیرکانه به کار ببرد که بتواند با ایجاد اعتبار و قدرت کافی، خود را از گزند حملات مخرب سایبری مصون بدارد.

در مقاله (دهقانی، ۱۳۹۷: ۲۵) نویسند معتقد است بر اساس نظریه رئالیسم ساختاری، کشورها در حوزه‌های مختلف از جمله سایبر، به تقویت قدرت تهاجمی خود ادامه خواهند داد تا بتوانند امنیت خود را ارتقاء بخشند. بر این اساس، فضای سایبر به سمت ناامنی روزافزون حرکت خواهند کرد. مشخصات فضای سایبر تفاوت زیادی با فضای سنتی دارد و ضروری است تغییراتی متناسب با این موضوع در بازدارندگی اعمال شود تا بتواند در محیط جدید قابلیت کاربرد پیدا کند. از مهم‌ترین تغییرات مورد نیاز، می‌توان به لزوم استفاده از چهار سازوکار تلافی، انکار، گرفتارسازی و هنجار استفاده نمود.

در مقاله (ملائی، ۱۳۹۷: ۱٦۸) قدرت سایبری به عنوان عنصر تعیین کننده در ایجاد بازدارندگی معرفی شده و عنوان شده است حتی در یک وضعیت ایده‌آل بازدارنده بایستی با داشتن برتری در قدرت سایبری همیشه گزینه‌های اقدام متقابل یا اقدام‌های لازم برای مهار را داشته باشد تا بتواند بازدارندگی را تأمین نماید. در مقاله بر اساس بهره‌های کسب شده در نتیجه اجرای راهبردهای متقابل در بازی بازدارندگی در فضای سایبر، پنج وضعیت منازعه، توازن، سلطه بازدارنده، سلطه تهدیدکننده و ضعف متقابل معرفی شده است. توازن، ضعف متقابل و سلطه بازدارنده (به‌شرط خویشتن‌داری وی)، وضعیت‌هایی هستند که بازدارندگی را به همراه خواهند داشت.

متولیان بازدارندگی در اسناد دیگر کشورها: در این بخش به بررسی اسناد راهبردی کشورها که در دسترس بوده‌اند از منظر بازدارندگی خواهیم پرداخت و اینکه از نگاه کشورها به‌طور خاص چه نهادهایی برای حصول اهداف بازدارندگی مورد توجه قرار گرفته است. وزارت دفاع آمریکا با همکاری سایر سازمان‌های دولت ایالات‌متحده، مسئول دفاع از کشور میزبان و منافع ایالات‌متحده در برابر حملات است، این حملات ممکن است در فضای مجازی رخ دهد. هدف این راهبرد، هدایت توسعه نیروهای سایبری وزارت دفاع آمریکا و تقویت دفاع سایبری و موضع بازدارندگی سایبری است. این تمرکز بر ایجاد قابلیت‌های سایبری و سازمان جهت سه مأموریت سایبری وزارت دفاع تمرکز دارد: اول بایستی از شبکه‌ها، سیستم‌ها و اطلاعات خود دفاع کند، دوم باید آماده دفاع از ایالات‌متحده و منافع آن در برابر حملات سایبری در مورد پیامدهای مهم باشد و سوم وزارت دفاع باید قادر به ارائه قابلیت‌های یکپارچه سایبری برای پشتیبانی از عملیات نظامی و برنامه‌های احتمالی باشد (نایبی‌پور، ۱۳۹۷: ۳۵-۳۲). وزارت دفاع باید در همکاری با ادارات و

سازمان‌های دیگر، متحدان و شرکای بین‌المللی، دولت‌های محلی و مهم‌تر از همه، بخش خصوصی، در جهت موفقیت‌های مأموریت‌های خود اقدام کند (همان، ۲۵).

در مطالعه (همان، ٤٧-٤٨) راهکارهایی شامل: بیان سیاست‌های سایبری، اعلام رسمی، عوامل قابل توجه هشدارهای نظامی- دفاعی، رویه‌های مؤثر پاسخ و انعطاف‌پذیری کلی شبکه، توانائی اعلام و نشان دادن توانائی‌های واکنش سریع جهت جلوگیری از نفوذ دشمن، توسعه قابلیت‌های دفاعی مؤثر به انکار یک حمله احتمالی، تقویت انعطاف‌پذیری کلی سیستم‌ها جهت مقاومت در برابر حملات، داشتن اطلاعات هوشمندانه، قابلیت‌های هشداردهنده جهت کاهش عوامل نامحدود در فضای مجازی، افزایش اعتماد به نفس، شناسایی (اسناددهی)، همکاری نزدیک با بخش خصوصی و سایر نهادهای دولتی و از جمله راهکارهای تنبیهی شامل اقدامات دیپلماتیک، اقدامات قانونی و تحریم‌های اقتصادی برای تحقق بازدارندگی اشاره شده است.

فرماندهی راهبردی ایالات‌متحده[۱] یکی از ده فرماندهی متحد در وزارت دفاع آمریکا می‌باشد. مسئولیت فرماندهی راهبردی، بازدارندگی راهبردی، ضربه جهانی و اداره کردن شبکه اطلاعات جهانی وزارت دفاع می‌باشد. فرماندهی راهبردی همچنین قابلیت‌های پشتیبانی برای دیگر فرماندهی‌های رزمی شامل هشدار راهبردی، دفاع موشکی یکپارچه، فرماندهی جهانی، ارتباطات، رایانه‌ها، تجسس، نظارت و شناسایی (***C٤ISR***) را فراهم می‌سازد. این فرماندهی پویا رهبری ملی منابع متحد را برای فهم بهتر تهدیدات در سراسر جهان و ابزاری برای پاسخ سریع به این تهدیدات می‌باشد. در پایگاه اطلاع‌رسانی[۲] این فرماندهی به عنوان اولویت‌های این فرماندهی اعلام شده است که اگر بازدارندگی شکست بخورد ما برای ارائه پاسخ قاطع آماده هستیم و این کار را با نیروهای آماده رزم، آموزش دیده، مجهز و مقاوم انجام خواهیم داد.

در مطالعه (ساوره‌درودی، ۱۳۹۷: ۵۲-۳۸) ساختار سازمانی ملی برای امنیت سایبری و دفاع سایبری در رژیم صهیونیستی در پنج بخش شامل: ۱- مدیریت سیاسی و راهبردی و هماهنگی امنیت ملی سایبری، ۲- مدیریت هماهنگی رویداد سایبری در راستای اشتراک‌گذاری اطلاعات داخلی و بین‌المللی و آگاهی بخشی شامل ***CERT*** ها و پلیس، ۳- حمایت از زیرساخت‌های حیاتی

۱- USSTRATCOM

۲- http://www.stratcom.mil/About/Mission/

و مدیریت بحران، ٤- دفاع سایبری نظامی و اطلاعات سایبری و ٥- مشارکت بخش خصوصی و همکاری میان دانشگاه و بخش کسب‌وکار معرفی شده است.

در سند راهبردی انگلیس (***HM-Government,*** ۲۰۱٦:۹) بازدارندگی در کنار دفاع و توسعه یکی از اهداف دستیابی به راهبرد امنیت سایبری ملی عنوان شده است. در این سند آمده است ما اقدامات خصمانه علیه خودمان را کشف، بازرسی و مختل می‌کنیم و متجاوزان را تحت تعقیب و پیگرد قانونی قرار خواهیم داد. همچنین برای انجام اقدامات لازم ابزارهای آفندی در فضای سایبر در اختیار داریم. مواردی چون کاهش جرائم سایبری، مقابله با بازیگران خارجی متخاصم، جلوگیری از تروریسم، ارتقاء قابلیت‌های مقتدرانه[1] آفند سایبری و رمزنگاری از موضوعاتی هستند که در بخش بازدارندگی مورد تأکید قرار گرفته است (***HM-Government,*** ۲۰۱٦: ٤٦-٥۲). در سند راهبردی استرالیا درباره بازدارندگی می‌نویسد (***Commonwealth of Australia,*** ۲۰۱٦:۲۸): برای کشف، بازداری و پاسخ بهتر به فعالیت‌های سایبری مخرب، اطلاعات تهدیدات سایبری باید به صورت بلادرنگ، در داخل و بین بخش‌های عمومی و خصوصی به اشتراک گذاشته شود. در این سند اشاره می‌شود با داشتن اطلاعات واحد برای شکل‌دهی تصویر تهدید و با ترکیب دانشمان می‌توانیم به صورت جامع تهدیدات امنیت سایبری استرالیا را و چگونگی مقابله با آن‌ها را درک کنیم. تحویل مجرمان به دست عدالت نیز به همان اندازه درک تهدیدات بسیار مهم است. قابلیت‌های آفند و پدافند سایبری، استرالیا را برای بازداری و پاسخ به تهدیدات حملات سایبری توانمند خواهد ساخت. استرالیا تمایل دارد هرگونه اقدام استفاده شده در بازداری و پاسخ به فعالیت‌های سایبری مخرب با قواعد نظم بین‌المللی و تعهد ما به قوانین بین‌المللی سازگار باشد.

در مطالعه (***Rosenzweig,*** ۲۰۱۰:۲٤۷) نویسنده اشاره دارد برای توسعه ساختار بازدارندگی، شناسایی زیردسته‌هایی از فعالیت‌های بازدارندگی سایبری بالقوه به‌منظور اندازه‌گیری سودمند ساختار و فرآیندهای موجود مفید می‌باشد. در حوزه انکاری می‌توان حداقل سه نوع متمایز فعالیت رو شناسایی کرد: ۱- دفاع سایبری، فعالیت‌های کلاسیک امنیت سایبری شامل کشف و جلوگیری از نفوذ و حملات سایبری، ۲- انعطاف‌پذیری (بازگشت‌پذیری) سایبری، فعالیت‌های مرتبط با تقویت شبکه‌های سایبری به‌طوری‌که حتی حملات موفق به خاطر افزونگی و قابلیت تعمیر نهادینه شده در سیستم، تأثیر کمتری داشته باشند، ۳- تضمین سامانه‌های سایبری، فعالیت‌های دلگرم‌کننده

۱- Sovereign

و پشت‌گرمی، از اینکه سیستم‌های سایبری مورد استفاده مورد هدف نفوذ و کنترل خارجی نیستند. به همین ترتیب به صورت مفهومی حداقل دو فعالیت متمایز در حوزه تنبیهی نیز مورد توجه هستند: ۱- حملات سایبری، فعالیت‌های مرتبط با واکنش به حملات سایبری شامل عمل سایبری تلافی جویانه (پیش‌دستانه)، ۲- واکنش غیرسایبری، فعالیت‌هایی که در واکنش به حملات سایبری انجام می‌شود، اما ماهیت سایبری ندارند (حملات نیروهای نظامی غیرسایبری). همه این فعالیت‌ها به یک ساختاری در سطح راهبردی نیاز دارد تا هماهنگی‌های سایبری را فراهم سازد.

فعالیت‌های مختلفی برای ایجاد بازدارندگی در کشورها مورد توجه بوده است که از جمله این فعالیت‌ها می‌توان به مواردی چون دفاع، یکپارچه‌سازی، پشتیبانی، همکاری، هماهنگی، انعطاف‌پذیری، بیان سیاست‌ها، واکنش سریع، هشداردهی، شناسایی، تجسس، نظارت، هماهنگی، اشتراک‌گذاری، آفند، پدافند، رمزنگاری، کشف و واکنش غیرسایبری اشاره کرد. از منظر متولیان در کشور در اسناد وزارت دفاع، ارتش، نیروهای مسلح و فرماندهی‌های راهبردی در یک سطح راهبردی و کلان ملی مورد تأکید بوده است. در زمان انجام این تحقیق بر اساس بررسی‌های به‌عمل‌آمده در اسناد رسمی، سندی مبنی بر تعریف و ترسیم چارچوبی از متولیان تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری یافت نشده است و مواردی که به صورت بخشی یا موردی مطرح بودند نیز در این بخش مورد بررسی قرار گرفت. هرچند نهادهای مختلفی بر اساس مأموریت‌ها و وظایف سازمانی فرآیندهایی را در راستای بازدارندگی تدوین و اجرا می‌نمایند، لیکن برای تعریف نهادهای مورد نیاز این فرآیندها و ارتباط آن‌ها با یکدیگر، مطالعه مشخصی صورت نگرفته است.

روش تحقیق:

حصول نهادهای تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و سطح‌بندی آن‌ها مبتنی بر مطالعات ادبیات تحقیق، اسناد بالادستی و مطالعات تطبیقی و با استفاده از روش‌های تجزیه و تحلیل مدلسازی امکان پذیر خواهد بود؛ بنابراین می‌توان نتیجه گرفت که نوع پژوهش در این زمینه توسعه‌ای خواهد بود. از طرف دیگر پژوهش حاضر در پی ارائه الگویی برای رفع نیاز کشور می‌باشد بنابراین پژوهش از این منظر کاربردی محسوب گردیده و در مجموع توسعه ای- کاربردی خواهد بود.

سپس با استفاده از روش مدل‌سازی ساختاری تفسیری[۱] میزان تأثیر متغیرهای مستقل بر متغیر وابسته بر اساس نظر خبرگان مورد سنجش قرار گرفت. از منظر قلمرو مکانی، این تحقیق در فضای سایبر جمهوری اسلامی ایران در نظر گرفته شده و به لحاظ موضوعی هدف اصلی صرفاً رسیدن به متولیان مورد نیاز برای کارکرد صحیح فرآیند ایجاد قدرت بازدارندگی و پیشگیری از حملات و تهدیدات سایبری در نظام دفاع سایبری در سطح راهبردی می‌باشد.

تعریف و تبیین حدود جامعه آماری در تحقیق کیفی بر اساس مواردی همچون مسئله تحقیق، ضرورت موضوع و ویژگی‌های آن مشخص می‌شود. نمونه‌گیری در تحقیقات کیفی به صورت غیرتصادفی و هدفمند است و ناظر به خبرگان این عرصه است. نمونه‌گیری در روش داده بنیاد تا آن‌جایی ادامه پیدا می‌کند که یک کفایت نظری حاصل شود. جامعه آماری مورد نظر در این تحقیق عبارتند از اساتید عضو هیأت علمی دانشگاه‌های متخصص در حوزه (امنیت فضای) سایبر، پژوهشگران مراکز پژوهشی و مدیران و متصدیان اجرایی که در حوزه فناوری اطلاعات و فضای سایبری کشور فعال هستند. در تحقیقات کیفی نمونه‌گیری تا حد اشباع صورت می‌گیرد اما توصیه شده است که در ابتدا حداقلی از تعداد نمونه در طرح تحقیق در نظر گرفته شود و به‌تدریج در حین انجام تحقیق احتمال افزایش این تعداد وجود دارد (***Patton,*** ۲۰۰۲).

برای آزمون فرضیه در روش پژوهش موردی، حجم نمونه بایستی حداقل ۳۰ نفر باشد. با توجه به اینکه متخصصین حوزه امنیت سایبر که دارای تجربه کافی در موضوع این تحقیق باشند محدود است لذا در جلسات گروه مطالعاتی، تصمیم به تمام شمار بودن جامعه آماری گرفته شد. از منظر روش نمونه‌گیری به منظور شناسایی جامعه آماری از روش گلوله برفی[۲] (زنجیره‌ای یا شبکه‌ای) که یکی از شایع‌ترین روش‌های نمونه‌گیری هدف‌مند در تحقیقات کیفی به‌شمار می‌آید، استفاده می‌شود. محقق در این روش مشارکت‌کنندگانی را انتخاب می‌کند و از طریق آن‌ها و با توجه به ویژه‌گی‌های مورد نظر به مشارکت کنندگان بعدی می‌رسد و در این راستا نیز گلوله برفی با پرسش از شماری از افراد در خصوص موضوع مورد تحقیق، بزرگ و بزرگ‌تر می‌شود تا جایی که اشباع اطلاعاتی پیرامون موضوع مورد مطالعه با استفاده از خبرگان به دست می‌آید (***Patton,*** ۲۰۰۲).

۱- Interpretive Structural Modelling
۲-Snowball Method

روش تجزیه و تحلیل: بعد از مطالعه مبانی نظری، اسناد بالادستی و مطالعات تطبیقی با اسناد در اختیار دیگر کشورها گام بعد دستیابی به ارتباطات فی‌مابین نهادها (متولیان) جهت تحقق اجرای فرآیندها است، بنابراین با استفاده از روش مدلسازی ساختاری- تفسیری و مقایسه‌ای زوجی مبتنی بر نظر خبرگان، تأثیرگذاری متولیان نظام دفاع سایبری بر یکدیگر در فرآیند بازدارندگی مورد بررسی قرار گرفت. بعد از احصاء متولیان پیشنهادی اولیه در قالب جلسات تجزیه و تحلیل و مصاحبه، در نهایت در مورد اثربخشی ۱٤ نهاد که در جدول شماره (۱) فهرست شده‌اند اشباع نظری حاصل گردید.

بررسی اثرگذاری متولیان بر یکدیگر: بعد از جمع‌آوری ماتریس‌های اظهار نظر خبرگان برای تأثیرگذاری و تأثیرپذیری متولیان مؤثر بر یکدیگر، درایه‌های ماتریس نظیر به نظیر با یکدیگر جمع می‌شوند که در جدول (۲) ماتریس حاصل جمع نمایش داده شده است. بعد از حاصل شدن ماتریس مجموع، در صورتیکه بزرگتر مساوی پنجاه درصد از خبرگان یک اثرگذاری را تأیید کرده باشند آن اثرپذیری مورد پذیرش قرار گرفته و در ماتریس دستیابی درایه متناظر، با مقدار ۱ نشان داده شده است. این ماتریس در جدول شماره (۳) نشان داده شده است. در ماتریس دستیابی نهائی مقادیر حاصل از جمع درایه‌های هر سطر و ستون محاسبه می‌شود. این مقادیر در جدول تعین موقعیت (شماره (٤)) مورد استفاده قرار می‌گیرد تا توان تأثیرگذاری و تأثیرپذیری متولیان بر یکدیگر اندازه‌گیری شود.

جدول شماره (۲): ماتریس حاصل جمع اظهارنظر خبرگان در رابطه با تأثیرگذاری خبرگان بر یکدیگر

نهاد		N۱	N۲	N۳	N٤	N٥	N٦	N۷	N۸	N۹	N۱۰	N۱۱	N۱۲	N۱۳
متولی سیاست‌گذاری حوزه امنیت سایبر	N۱	۱۰	۹	۹	۹	۸	۷	۸	۹	۹	۷	۸	۹	۷
متولی فرماندهی سایبری و تعیین وضعیت	N۲	٤	۱۰	٦	۹	۹	۹	۹	۹	۹	۷	۸	۹	۸
متولی تدوین قوانین و مقررات سایبری	N۳	٥	٥	۱۰	۷	۹	۸	۷	۷	۸	٦	۸	۸	۸
متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N٤	۳	۲	۲	۱۰	٥	۹	۷	٥	۷	۳	٥	٦	٦
متولی امور بین‌الملل و دفاع سایبری کشورهای اسلامی	N٥	٤	۳	٤	٥	۱۰	٦	۷	٤	٦	۳	٦	٥	٥
متولی مراکز عملیات امنیت شبکه و پاسخگویی	N٦	۱	۱	۲	٦	٤	۱۰	٥	٤	٦	۳	٤	۷	٥

متولی مقابله با جرائم سازمان‌یافته و تروریسم سایبری	N۷	۳	۲	۳	۸	٦	٦	۱۰	٦	٥	٦	۳	۷	٦
متولی هماهنگی امنیت سایبری قوای سه‌گانه	N۸	۲	۳	٤	٦	٦	٤	٦	٦	۱۰	٦	٥	٦	۸
متولی حفاظت از زیرساخت‌های ملی	N۹	۲	۲	۳	۹	۷	۹	۸	٤	۱۰	٦	٥	٦	٦
متولی نظارت و ارزیابی	N۱۰	٥	۷	۷	٦	٦	۸	۸	٥	۸	۱۰	۸	۸	۸
متولی رصد، پایش تهدیدات و اشتراک‌گذاری	N۱۱	٤	۳	۳	۷	۷	۹	۹	٥	٥	٤	۱۰	٥	٦
متولی تحقیقات آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری	N۱۲	۳	٤	۳	٦	٦	۸	۷	٥	٥	۳	۳	۱۰	۱۰
متولی رمز ملی و تصدیق هویت مجازی	N۱۳	۲	٤	۲	٦	٦	۸	۸	٦	٥	۳	٤	۸	۱۰
نهاد مدیریت محتوای سایبری و رسانه‌ها	N۱٤	۲	٤	۲	٤	٦	٦	۷	٥	۳	۳	٦	۳	۳

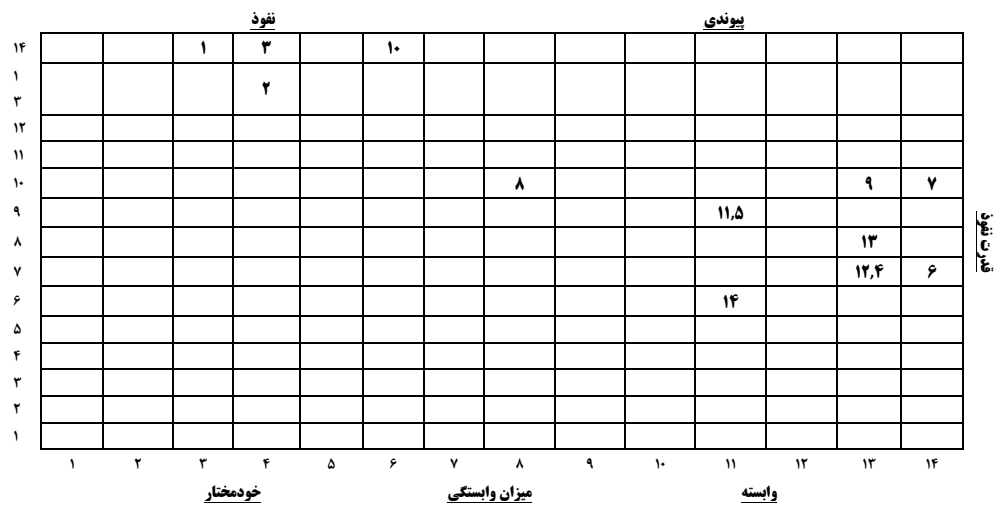
جدول (۳): ماتریس دستیابی نهائی

نهاد		N۱	N۲	N۳	N٤	N٥	N٦	N۷	N۸	N۹	N۱۰	N۱۱	N۱۲	N۱۳	N۱٤	
متولی سیاست‌گذاری حوزه امنیت سایبر	N۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱٤
متولی فرماندهی سایبری و تعیین وضعیت	N۲	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۳
متولی تدوین قوانین و مقررات سایبری	N۳	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱٤
متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N٤	۰	۰	۰	۱	۰	۱	۱	۰	۱	۰	۱	۱	۱	۰	۷
متولی امور بین‌المللو دفاع سایبری کشورهای اسلامی	N٥	۰	۰	۰	۱	۱	۱	۱	۰	۱	۰	۱	۱	۱	۱	۹
متولی مراکز عملیات امنیت شبکه و پاسخگویی	N٦	۰	۰	۰	۱	۰	۱	۱	۰	۱	۰	۰	۱	۱	۱	۷
متولی مقابله با جرائم سازمان‌یافته و تروریسم سایبری	N۷	۰	۰	۰	۱	۱	۱	۱	۱	۱	۰	۱	۱	۱	۱	۱۰
متولی هماهنگی امنیت سایبری قوای سه‌گانه	N۸	۰	۰	۰	۱	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۱
متولی حفاظت از زیرساخت‌های ملی	N۹	۰	۰	۰	۱	۱	۱	۱	۰	۱	۱	۱	۱	۱	۱	۱۱
متولی نظارت و ارزیابی	N۱۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱٤
متولی رصد، پایش تهدیدات و اشتراک‌گذاری	N۱۱	۰	۰	۰	۱	۱	۱	۱	۱	۱	۰	۱	۱	۱	۱	۹

متولی تحقیقات، آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری	$N'_{۲}$	۰	۰	۰	۱	۱	۱	۱	۱	۰	۱	۱	۰	۰	۱	۷
متولی رمز ملی و تصدیق هویت مجازی	$N'_{۳}$	۰	۰	۰	۱	۱	۱	۱	۱	۱	۰	۰	۱	۱	۰	۸
نهاد مدیریت محتوای سایبری و رسانه‌ها	$N'_{٤}$	۰	۰	۰	۰	۱	۰	۱	۱	۱	۱	۰	۰	۰	۱	٦
		۳	٤	٤	۱۳	۱۱	۱٤	۱٤	۸	۱۳	٦	۱۱	۱۳	۱۳	۱۱	

تعیین توان تأثیرگذاری- تأثیرپذیری متغیرها: با استفاده از ماتریس تعیین موقعیت، موقعیت هریک از متولیان در چهار وضعیت پیوندی، نفوذ، خودمختار و وابسته تعیین می‌گردد. نهادهای فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری با توجه به ماتریس تحلیل در هریک از این موقعیت‌ها توزیع می‌شوند و هرچقدر موقعیت آن‌ها به منطقه پیوندی نزدیک باشد نقش نهاد مزبور با اهمیت‌تر و هرچقدر به منطقه خودمختار نزدیک باشند نقش آن‌ها کمرنگ‌تر خواهد بود و می‌توان آن‌ها را از فرآیند حذف نمود.

جدول (٤): جدول تعیین موقعیت



در نتیجه انجام محاسبات تعیین موقعیت که در جدول شماره (٤) نشان داده شده است، هیچ نهادی در منطقه خودمختار قرار نگرفته است؛ بنابراین همه متولیان در فرآیند ایجاد قدرت بازدارندگی نقش دارند و هیچ نهادی کنار گذاشته نخواهد شد.

سطح‌بندی متولیان: یکی دیگر از اقداماتی که در تجزیه و تحلیل مدل می‌بایست انجام شود سطح‌بندی نهادهای فرآیند می‌باشد. برای تعیین روابط و سطح‌بندی معیارها باید مجموعه خروجی‌ها و مجموعه ورودی‌ها برای هر متولی از ماتریس دستیابی نهائی استخراج شود. مجموعه خروجی‌ها شامل خود متولی و متولیانی است که از آن تأثیر می‌پذیرد. مجموعه ورودی‌ها شامل خود متولی و متولیانی است که در ستون‌های ماتریس دستیابی نهائی جدول (۳) مقدار یک دارند خروجی‌ها شامل خود متولی و متولیانی است که در سطرهای ماتریس دستیابی نهائی مقدار یک دارند. در گام بعد برابر جدول شماره (۵) اشتراک مجموعه‌های ورودی و خروجی به‌دست می‌آید. متولی که مجموعه اشتراک دو مجموعه ورودی و خروجی آن با مجموعه خروجی برابر باشد، به عنوان سطح اول در نظر گرفته خواهد شد و این نهاد از فرآیند سطح‌بندی کنارگذاشته خواهد شد و دوباره این اعمال برای سطح‌بندی‌های بعدی انجام می‌شود تا آخرین متولی یا متولیان سطح آن تعیین شود. در جدول شماره (۵) سطح بندی متولیان فرآیند ایجاد قدرت بازدارندگی نمایش داده شده است.

جدول (۵): ماتریس سطح‌بندی ورودی‌ها و خروجی‌های فرآیند ایجاد قدرت بازدارندگی

فرآیند	معیار (سطح ۱)	ورودی‌ها	خروجی‌ها	مشترک	سطح
۱	متولی سیاست‌گذاری حوزه امنیت سایبر	۱	۱	۱	۷
۲	متولی فرماندهی سایبری و تعیین وضعیت	۱-۲	۲	۲	٦
۳	متولی تدوین قوانین و مقررات سایبری	۱-۲-۳	۳	۳	٥
٤	متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	۱-۲-۳-٤-٦-۷-۸-۹-۱۰-۱۱-۱۲-۱۳	٤-٦-۷-۹-۱۲-۱۳	٤-٦-۷-۹-۱۲-۱۳	۱
٥	متولی امور بین‌الملل و دفاع سایبری کشورهای اسلامی	۱-۲-۳-٥-۹-۱۰-۱۱-۱۲-۱۳	٥-۹-۱۱	٥-۹-۱۱	۲
٦	متولی مراکز عملیات امنیت شبکه و پاسخگویی	۱-۲-۳-٥-٦-۷-۸-۹-۱۰-۱۱-۱۲-۱۳-۱٤	٦-۹-۱۲-۱٤	٦-۹-۱۲-۱٤	۱
۷	متولی مقابله با جرائم سازمان‌یافته و تروریسم سایبری	۱-۲-۳-٥-۷-۸-۹-۱۰-۱۱-۱۲-۱۳-۱٤	٥-۷-۹-۱۱-۱۲-۱۳-۱٤	٥-۷-۹-۱۱-۱۲-۱۳-۱٤	۱
۸	متولی هماهنگی امنیت سایبری قوای سه‌گانه	۱-۲-۳-۸	۸	۸	٤
۹	متولی حفاظت از زیرساخت‌های ملی	۱-۲-۳-۸-۹-۱۰	۹	۹	۳
۱۰	متولی نظارت و ارزیابی	۱-۲-۳-۱۰	۲-۳-۱۰	۲-۳-۱۰	٤
۱۱	متولی رصد، پایش تهدیدات و اشتراک‌گذاری	۱-۲-۳-۸-۱۰-۱۱	۱۱	۱۱	۳
۱۲	متولی تحقیقات، آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری	۱-۲-۳-۸-۹-۱۰-۱۲-۱۳	۱۲-۱۳	۱۲-۱۳	۲
۱۳	متولی رمز ملی و تصدیق هویت مجازی	۱-۲-۳-۸-۹-۱۰-۱۱-۱۳	۸-۱۳	۸-۱۳	۲
۱٤	نهاد مدیریت محتوای سایبری و رسانه‌ها	۱-۲-۳-٥-۸-۱۰-۱۱-۱٤	٥-۱۱-۱٤	٥-۱۱-۱٤	۱

مدل مفهومی تحقیق:

فرآیندهای نظام دفاع سایبری: مدل مفهومی تحقیق در قالب جدول (٦) و شکل (١) به همراه ارتباط بین نهادها در هفت سطح برای ١٤ نهاد ارائه می‌شود. برای رسیدن به این مدل از روش *ISM* استفاده شده است که در بخش تجزیه و تحلیل به بیان جزئیات آن پرداخته شد. در این مدل ١٤ نهاد متولی در فرآیند ایجاد قدرت بازدارندگی در سطوح هفتگانه سطح‌بندی شده‌اند.

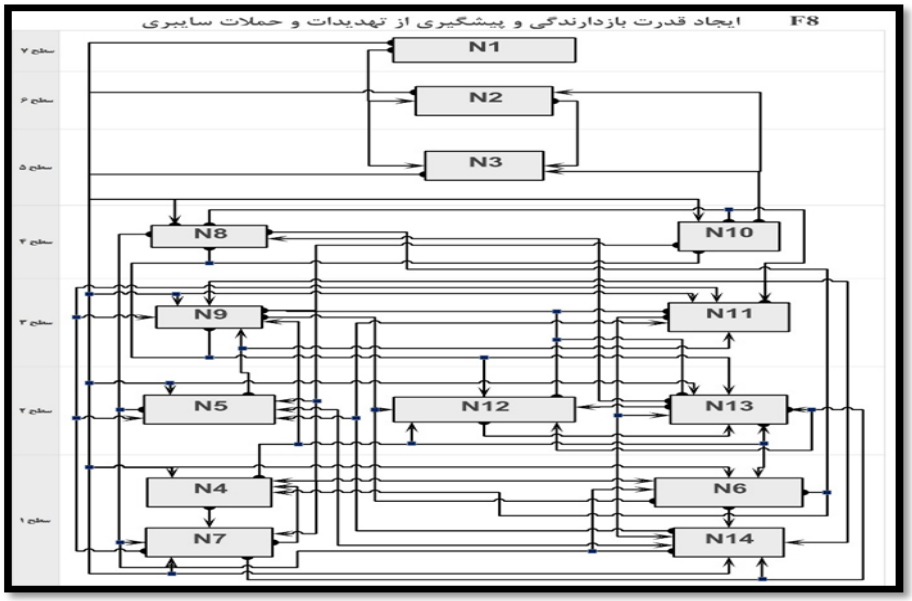
جدول (٦): نهادهای مؤثر در اجرای فرآیند ایجاد قدرت بازدارندگی

سطح	متولی
هفتم	سیاست گذاری حوزه امنیت سایبر (N١)
ششم	فرماندهی سایبری و تعیین وضعیت (N٢)
پنجم	تدوین قوانین و مقررات سایبری (N٣)
چهارم	هماهنگی امنیت سایبری قوای سه‌گانه (N٨) و نظارت و ارزیابی (N١٠)
سوم	حفاظت از زیرساخت‌های ملی (N٩) و رصد، پایش تهدیدات و اشتراک‌گذاری (N١١)
دوم	امور بین‌الملل و دفاع سایبری کشورهای اسلامی (N٥)، تحقیقات، آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری (N١٢) و رمز ملی و تصدیق هویت مجازی (N١٣)
اول	امنیت فضای سایبر در صنعت کشور و بیمه کشور (N٤)، مراکز عملیات امنیت شبکه و پاسخگویی (N٦)، مقابله با جرائم سازمان یافته و تروریسم سایبری (N٧) و مدیریت محتوای سایبری و رسانه‌ها (N١٤)

هرچه سطح یک متولی در مدل ارائه شده بالاتر می‌رود، میزان تأثیرگذاری آن متولی بر دیگر متولیان بیشتر می‌شود. به عنوان مثال نهادهای متولی در سطح اول بیشترین تأثیر را از دیگر متولیان خواهند داشت. متولیان سطوح پائین‌تر دارای وابستگی بیشتر به نسبت متولیان سطوح بالاتر دارند و متولیان سطوح بالاتر (سطح هفتم) دارای قدرت نفوذ بیشتری بر دیگر متولیان می باشند. این

سطوح و تبیین آن در بخش تجزیه و تحلیل با استفاده از جدول تعیین موقعیت بر اساس ورودی و خروجی هر نهاد انجام شده است.

شکل (۱): مدل مفهومی متولیان تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری



نتیجه‌گیری:

در پایان نتایج تحقیق نشان می‌دهد که کلیه ١٤ نهاد مورد بررسی بر روی فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری تأثیرگذار بوده و جهت حصول اهداف بازدارندگی مورد نیاز می‌باشند. در گام دوم، با توجه به تأثیرگذاری نهادهای متولی بر روی یکدیگر، مبتنی بر ورودی و خروجی هر نهاد، سطح تأثیرگذاری هر نهاد تعیین شده است. نهادهای سطح بالاتر قدرت نفوذ بیشتری بر دیگر نهادها دارند و دارای قدرت تصمیم‌گیری بالاتری هستند و نهادهای سطوح پائین‌تر وابستگی بیشتری به دیگر نهادها دارند. فرآیند «ایجاد قدرت بازدارندگی

و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری» شامل زیرفرآیندهای ۱- شناسایی دارایی‌های ارزشمند تهدیدکننده و بازدارنده، ۲-شناسایی بازیگر یا بازیگران تهدیدکننده، ۳-شناسایی سناریوهای تهدید و برآورد اعتبار آن‌ها، ٤- شناسایی آسیب‌پذیری‌های بازدارنده و تهدیدکننده و اندازه‌گیری میزان آسیب‌پذیری، ٥- اندازه‌گیری مخاطرات متوجه تهدیدکننده و بازدارنده، ٦- تدوین اهداف و سیاست‌های بازدارندگی، ۷- تدوین راهبردهای بازدارندگی بر اساس قابلیت‌ها و توانمندی‌های انکاری، تنبیهی و وابستگی، ۸- رصد علامت‌های ظاهرشده و کشف‌شده تهدیدکننده بر اساس تحرکات، رفتار و گفتار در فضای سایبری و حقیقی خود و حریف، ۹- محاسبه بهره و منافع بازیگران و تحلیل و تعیین وضعیت بر اساس شرایط بازدارندگی، ۱۰-هشداردهی و اطلاع رسانی و ۱۱-طراحی سازوکارهای جدید می‌باشد؛ بنابراین هر یک از نهادهای وضع موجود کشور می‌بایست در تناظر با متولیان چهارده‌گانه نتیجه تحقیق در راستای ایجاد قدرت بازدارندگی مأموریت‌های خود را بروز رسانی نمایند و در صورتیکه نهاد متناظری وجود ندارد ایجاد و مأموریت‌های آن تدوین گردد.

کارهای آینده: بررسی وضع موجود کشور در تناظر با نهادهای مطلوب احصاء شده تحقیق و احصاء کاستی‌ها و تدوین ساختار بهینه از جمله موضوعاتی است که می‌تواند در آینده مورد پژوهش قرار گیرد. در تحقیقات آینده بایستی این موضوع مورد توجه قرارگیرد که آیا متولیان موجود کشور قابلیت‌ها و توانمندی‌های لازم را برای ایجاد قدرت بازدارندگی دارند؟ بازدارندگی نیازمند یک برگ برنده یا راهبردی مؤثر و معتبر می‌باشد که روکردن آن بتواند دشمن را متقاعد نماید که از تصمیم خود منصرف گردد؛ بنابراین از منظری دیگر احصاء مؤلفه‌های راهبرد بازدارندگی دفاع سایبری کشور از دیگر موضوعاتی است که می‌تواند در راستای تکمیل حوزه مطالعاتی بازدارندگی در دفاع سایبری کشور مدنظر قرارگیرد. این مؤلفه‌ها می‌تواند شامل جزئیات سیاست‌گذاری، قوانین، بیانیه‌ها، قابلیت‌ها و توانمندی‌هایی چون آگاهی موقعیتی، نفوذ، پایش، یکپارچه‌سازی دادگان، انکار (پدافند)، اقدام متقابل (آفند)، اقدامات تنبیهی، راهکارهای وابستگی مشترک، مکانیزم‌های تصمیم‌گیری، اعلام مواضع، اطلاع‌رسانی و هشداردهی و خروج از بحران باشد.

منابع:

- دهقانی، علی‌اصغر، (۱۳۹۷)، ***بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت های حیاتی آمریکا***، رهیافت‌های سیاسی و بین‌المللی.
- دولت‌آبادی باقری، علی، (۱۳۹۲)، ***نقش بازدارندگی در راهبرد نظامی ایران***، مجله سیاست دفاعی، سال بیست و دوم، شماره ۸۵، زمستان ۱۳۹۲، صفحات ۳۷-۸۷
- سازمان پدافند غیرعامل، (۱۳۹۳)، ***سند راهبردی پدافند سایبری کشور***، ماهنامه پاپسا شماره اول، خردادماه.
- ساوره‌درودی، مصطفی؛ پوریانی، جابر، (۱۳۹۷)، ***امنیت سایبری در رژیم صهیونیستی***.
- قوانین کشور، (۱۳۹٤)، ***سیاست‌های کلی برنامه‌ی ششم***، ابلاغ رهبری به رئیس‌جمهور، قوانین کشور.
- ملائی، علی؛ کارگری، مهرداد؛ خراشادی‌زاده، محمدرضا، (۱۳۹۷)، ***الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها***، فصلنامه امنیت ملی دانشگاه عالی دفاع ملی، صفحات ۱٤۱-۱۷۲.
- ملائی، علی؛ محمدی، علی، (۱۳۹۲)، ***ارائه نظام رصد و پایش تهدیدات و حملات فضای سایبر با استفاده از معماری*** ISAC. فصلنامه نگرش امنیتی سال اول، شماره چهارم.
- نایبی‌پور، محمدرضا؛ خزائی، امید؛ حسینی، سیده‌زهره، (۱۳۹۷)، ***دیپارتمان مقابله با تهدیدات سایبری ایالات‌متحده آمریکا***، تهران: انتشارات پشتیبان.
- وحیدپور، حمید، (۱۳۹۲)، ***لازمه وجود توانمندی‌های سایبری پدافندی و تهاجمی به عنوان عوامل بازدارندگی***، Paper presented at the ششمین کنگره انجمن ژئوپلیتیک ایران پدافند غیرعامل مشهد.

- راهبرد سایبری وزارت دفاع آمریکا (۲۰۱۸)

https://media.defense.gov Retrieved from
-/۱-/۲۰۰۲۰٤۱٦٥۸/۱۷/Sep/۲۰۱۸https://media.defense.gov/
CYBER_STRATEGY_SUMMARY_FINAL.PDF/۱/۱

- راهبرد سایبری وزارت دفاع آمریکا (۲۰۱٥)

https://archive.defense.gov Retrieved from https://archive.defense.gov:
_cyber-۰٤۱٥/۲۰۱٥https://archive.defense.gov/home/features/
_dod_cyber_strategy_for_web.pdf ۲۰۱٥strategy/final_

- *Beidleman, Scott W. (۲۰۰۹). Defining and deterring cyber war. Retrieved from*
- *Commonwealth of Australia, Department of the Prime Minister and Cabinet. (۲۰۱٦). AUSTRALIA'S CYBER SECURITY STRATEGY. Enabling innovation, growth & prosperity.*
- *DIA_New_Zealand .(۲۰۱٤) .Risk Assessment process information security. Internal Affairs New Zealand government. Te Tari Taiwhenua.*
- *DOD_of_Belgian. (۲۰۱٤). Cyber Security Strategy for Defence. CST–Strategy-CyberSecurity-۰۰۱ Ed ۰۰۱ / Rev ۰۰۰ ۲۰۱٤/۰۹/۳۰:DEFENCE.Strategy Department.*
- *DOD_OF_USA. (۲۰۱۱). Department of defense strategy for operating in cyberspace. Department of defense*
- *FCR_Austria. (۲۰۱۳). Austrian Cyber Security Strategy. Federal Chancellery of the Republic of Austria.*
- *Goodman, Will. (۲۰۱۰). Cyber deterrence: Tougher in theory than in practice? Retrieved from*
- *Hausken, Kjell, & Zhuang, Jun. (۲۰۱۲). The timing and deterrence of terrorist attacks due to exogenous dynamics. Journal of the Operational Research Society, ٦۳(٦), .۷۳٥-۷۲٦*
- *HM-Government. (۲۰۱٦). National Cyber Security Strategy .۲۰۲۱-۲۰۱٦*
- *Jensen, Eric Talbot .(۲۰۱۲) .Cyber Deterrence.*
- *Kesan, Jay P, & Hayes, Carol M. (۲۰۱۱). Mitigative counterstriking: Self-defense and deterrence in cyberspace. Harv. JL & Tech. ۲٥, .٤۲۹*
- *Kugler, Richard L. (۲۰۰۹). Deterrence of cyber attacks. Cyberpower and national security. ۳۲۰ ,*
- *Liles, Jonathan S, & Davidson, Janine. (۲۰۱۳). Modern Cyber Deterrence Theory: Norms, Assumptions and Implications.*
- *MOD_UK. (۲۰۱۱). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. London: MOD UK: Ministry of Defence (United Kingdom.(*
- *Moore, Ryan J. (۲۰۰۸). Prospects for cyber deterrence. Retrieved from*
- *Morgan, Patrick M. (۲۰۱۰). Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. Paper presented at the Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy.*
- *Mowbray, TJ. (۲۰۱۰). Solution architecture for cyber deterrence.*
- *Patton, Michael Quinn. (۲۰۰۲). Qualitative Research & Evaluation Methods.*

- *Payappalli, Vineet M, Zhuang, Jun & ,Jose, Victor Richmond R. (۲۰۱۷). Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts. Risk Analysis.*
- *Prime_Minister_of_France. (۲۰۱۵). FRENCH NatioNal digital security strategy. Courtesy translation. Foreword from Manuel Valls, Prime Minister of France, French national digital security strategy. Prime Minister of France.*
- *Rosenzweig, Paul. (۲۰۱۰). The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR US POLICY, National Research Council, Forthcoming.*
- *Taipale, KA. (۲۰۱۰). Cyber-deterrence. Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global*