الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها

علی ملائی[1]
مهرداد کارگری[2]
محمدرضا خراشادی زاده[3]

تاریخ دریافت:۱۳۹۶/۱۲/۱۶ تاریخ پذیرش: ۱۳۹۷/۰۲/۱۶

چکیده:

امروزه رشد هرچه بیشتر وابستگی‌های زندگی بشری به فضای سایبر، باعث شده است تا تهدیدات سایبری به زیرساخت‌های راهبردی مورد توجه دشمنان هر جامعه‌ای قرار بگیرد. حملات سایبری که در کشورهایی چون استونی، گرجستان و همچنین در ایران در گذشته رخ داده است به ما هشدار خواهد داد، آینده فضای سایبر عاری از حملات و تهدیدات دفاعی و امنیتی نخواهد بود؛ بنابراین بازدارندگی یکی از موضوعات اساسی در حوزه دفاعی- امنیتی هر کشور است. در این پژوهش ارائه الگویی از بازدارندگی در تأمین امنیت دارایی‌های سایبری مسئله اصلی است.

در این تحقیقِ اکتشافی، احصاء الگوی راهبردی بازدارندگی در فضای سایبر، بر اساس نظریه بازی‌ها هدف اصلی است و نظریه بازی‌ها در مدل‌سازی، تحلیل و حل مسئله به ما کمک خواهد کرد. این تحقیق از نوع کاربردی- توسعه ای است و از تجزیه و تحلیل توصیفی، استنباطی، آماری و مبتنی بر تحلیل ریاضیات نظریه بازی‌ها استفاده خواهیم کرد. در نهایت الگوی بازدارندگی در فضای سایبر با بهره‌گیری از بازی پویای علامت‌دهی با اطلاعات ناقص و تعادل نش راهبردهای مختلط در شش بعد و چهار مؤلفه اصلی وضع موجود، وضع مطلوب، تحلیل فاصله و برنامه اقدام معرفی می‌گردد. از منظر این الگو بازیگران تهدیدکننده و بازدارنده با توجه به بهره‌ای که در بازی به دست می‌آورند در پنج وضعیت منازعه، توازن، سلطه بازدارنده، سلطه تهدیدکننده و ضرر متقابل قرار می‌گیرند.

کلیدواژه‌ها: بازدارندگی، فضای سایبر، بازی علامت‌دهی، تعادل نش کامل، راهبردهای مختلط

۱- دانشجوی دوره دکتری مدیریت راهبردی امنیت فضای سایبر (نویسنده مسئول)- A.mollaei@sndu.ac.ir
۲- استادیار و عضو هیئت علمی دانشگاه تربیت مدرس- M_kargari@modares.ac.ir
۳- دانشیار و عضو هیئت علمی دانشگاه عالی دفاع ملی- Mr.khorashadi@sndu.ac.ir

مقدمه:

در کشور اسناد متنوعی از جمله:

۱- سیاست‌های کلی برنامه ششم توسعه،

۲- سند چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴،

۳- ابلاغ سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)»،

۴- احکام انتصاب شورای عالی فضای مجازی،

۵- سیاست‌های کلی نظام در امور پدافند غیرعامل،

۶- سند راهبردی پدافند سایبری کشور،

موضوع بازدارندگی را یکی از نیازهای اساسی تأمین امنیت کشور دانسته‌اند. طبیعتاً امنیت در فضای سایبر یکی از مؤلفه‌های اصلی امنیت ملی کشور است. امروزه با رشد هر چه بیشتر فضای سایبر و وابستگی‌های زندگی بشری به این حوزه فناوری، تهدیدات سایبری به زیرساخت‌های ملی نیز مورد توجه دشمنان هر جامعه‌ای قرار گرفته است. حملات سایبری که در کشورهایی چون استونی، گرجستان و همچنین در ایران در گذشته رخ داده است به ما هشدار خواهد داد، آینده فضای سایبر عاری از حملات و تهدیدات دفاعی و امنیتی نخواهد بود. بازدارندگی یکی از موضوعات اساسی در حوزه دفاعی- امنیتی هر کشور است. 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 پیاده‌سازی و اجرای سیاست‌های کلی فضای سایبر یکی از موضوعات پراهمیت و اساسی است.

نبود یک زبان و شیوه مناسب برای محاسبه روابط متغیرهای بازدارندگی در فضای سایبر، درک طرفین را از محیط و اتخاذ تصمیمِ مناسب را با مشکل مواجه خواهد ساخت و پیامدها را غیرقابل پیش‌بینی می‌سازد و دقت تصمیم‌گیری‌ها را پائین می‌آورد. بنابراین ممکن است طرفین را به یک جنگ سایبری سوق دهد، از این رو نبود الگوهای دانشی برای شفاف‌سازی مسائل پیش رو می‌تواند صدمات و خسارت‌هایِ جبران‌ناپذیری را به همراه داشته باشد. این الگو می‌بایست تبیین بهتری از شناخت و برآورد اعتبار تهدیدات ارائه نماید، مخاطرات هر تهدید را اشاره کند و بهینه-

ترین راهبردهای امنیتی و دفاعی سایبری را برای بازدارندگی پیشنهاد نماید تا راهبرد و تهدید متناسب و تأثیرگذار در پاسخ به دشمن فراهم گردد.

بازدارندگی در فضای سایبر یک حوزه تعارض بین تهدیدکننده و بازدارنده برای کسب منابع و منافع مورد نظر به وجود خواهد آورد و باعث خواهد شد، تصمیم بازیگران بر یکدیگر تأثیرگذار باشد. این شرایط از نگاه نظریه بازی‌ها نوعی بازی را بین بازیگران به وجود خواهد آورد. در یک بازی، تعاملاتی (روابط متقابل) برقرار است که می‌بایست در آن بین تصمیم دو طرف (بیشتر) وابستگی یا ارتباط متقابل وجود داشته باشد. به عبارت دیگر می‌توان گفت، هرگاه مطلوبیت، سود، درآمد، رفاه و هر آنچه فرد بازیکن به دنبال آن است، نه‌تنها متأثر از تلاش و تصمیم خود باشد بلکه تحت تأثیر (مثبت یا منفی) تلاش و تصمیم طرف دیگر نیز باشد، به آن بازی اطلاق می‌شود (عبدلی، ۱۳۹۲: ۲).

یک بازی، توصیفی از فعل و انفعالات راهبردی است که شامل تحمیل‌هایی روی اعمال بازیکنان و علاقه‌مندی‌های بازیکنان می‌شود و فقط مختص اعمالی که بازیکنان انجام می‌دهند نیست. یک راهکار یا راه‌حل توصیفی سیستمی از خروجی‌ها یا نتایج که ممکن است در یک خانواده از بازی‌ها ادغام شود، است. نظریه بازی‌ها، راهکارهای مناسبی را برای دسته‌ای از بازی‌ها پیشنهاد می‌کند و خصوصیات آن‌ها را تعیین می‌کند (*Osborne & Rubinstein, 1994: 2*).

تمامی موقعیت‌های تعارض‌آمیزی که در عمل رخ می‌دهند بسیار پیچیده‌اند و تحلیل آن‌ها به‌واسطه عوامل بسیاری پیش نمی‌رود. برای امکان‌پذیر بودن تحلیل ریاضی یک موقعیت، ضروری است که خود را از دست این عوامل درجه دو خلاص کنیم و یک مدل ساده شده و صوری از موقعیت بسازیم چنین مدلی را یک بازی خواهیم نامید (روشندل و طیب، ۱۳۷۳: ۶). رسم بر آن است که طرف‌های شرکت کننده را بازیکن و نتیجه یک رویارویی را «امتیاز» یا «پرداخت» یک بازیکن می‌خوانند. یک بازی ممکن است تصادم منافع دو یا چند حریف باشد (همان: ۱۳).

تحقیق‌های متنوعی در موضوع بازدارندگی در فضای سایبر صورت گرفته است. در تحقیق (*Mowbray, 2010: 58*) قابلیت‌های بازدارندگی سایبری در سطح راهبردی و فنی مورد توجه بوده است. فناوری‌هایی برای تولید اجزاء اصلی راهکار، پیش‌بینی شده‌اند و در نهایت نتایج به‌عنوان یک معماری مفهومی (مدل مرجع بازدارندگی)، مدل مفهومی حمله‌کننده و معماری مفهومی برای اسناددهی سریع ارائه شده است.

تحقیق (*Beidleman, 2009*) در روشی توصیفی و تحلیلی ارائه شده است که حملات سایبری در شرایطی خاص می‌توانند به‌عنوان عملی در جنگ به‌کار گرفته شوند. تعریف هنجارهای بین-المللی در فضای سایبر می‌تواند به بازدارندگی کمک کند. بازدارندگی برای دلسرد کردن تجاوزگر به‌کار می‌رود و پیشنهاداتی را برای محافظت از منافع ملی ارائه می‌کند. در تحقیق دیگری (*Moore, 2008*) 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 و خصوصیات بازدارندگی سایبری نیز تعیین شده‌اند. بازدارندگی انکار و بازدارندگی تنبیه، تکنیک‌ها و تعیین حد آستانه و توسعه سیاست‌های ملی مورد تحلیل و بررسی قرار گرفته است.

در تحقیق دیگری (*Rice, Butts, & Shenoi, 2011*) با عنوان «یک چارچوب علامت‌دهی برای بازدارندگی تجاوز سایبری» به‌صورت توصیفی بدون حل مدل، اجزاء چارچوب در سطح تکنیکال تشریح شده است. بدون فرموله‌سازی از حل مسئله و یا چگونگی حل تعادل بازی، دسته‌بندی علامت‌ها در بازی بازدارندگی انجام شده است و دسته‌بندی عمل‌های مدافع و دشمن از نگاه محقق در تحقیق ارائه شده است.

در (*Schramm, Alderson, Carlyle, & Dimitrov, 2012*) تحقیقی با عنوان مدل نظریه بازی‌ها از منازعه راهبردی در فضای سایبر، در قالب سؤال «چگونه می‌توان ارزش وارد شدن در منازعه سایبری را به‌وسیله نظریه بازی‌ها مدل‌سازی کرد؟» منازعه سایبری را به‌عنوان یک بازی دونفره با جمع صفر در زمان گسسته که هر بازیکن یک سوءاستفاده بر طبق یک فرآیند تصادفی کشف می-کند، در نظر گرفته شده است. مدل‌سازی ریاضی بازی با بازی جمع صفر با اطلاعات کامل و بررسی بازی مارکوف انجام شده و به‌طور ضمنی به بازدارندگی اشاره داشته و چارچوبی برای تحلیل منازعه سایبری آورده است. همچنین نشان داده است که در منازعه سایبری زمانِ انتظار اهمیت زیادی دارد و باید در مورد زمان حمله تصمیم‌گیری مناسب صورت گیرد.

در تحقیق (*Taquechel & Lewis, 2012*) مدلی ارائه شده است تا بتواند اندازه‌گیری نماید اینکه مهاجم تا چه حد از حمله منصرف شده است و چه حدی از کاهش مخاطره، در نتیجه اجرای بازدارندگی صورت گرفته است و هزینه‌ها و تأثیرات در اجرای بازدارندگی چه مقدار هستند؟ در تحقیق دیگری مدل بازی با پویایی‌های قطعی و پویایی‌های تصادفی در زمان‌بندی و

بازدارندگی حملات تروریستی ارائه شده است. مدافع یک دارایی را تحت حملات تکرار شونده کنترل می‌کند. هدف مدافع بازداری مهاجم است (*Hausken & Zhuang, 2012*).

این تحقیق قصد دارد با تکیه بر نظریه بازی‌ها به ارائه الگویی بپردازد که محیط تنازع سایبری متشکل از طرفین بازدارنده و تهدیدکننده را مدل‌سازی نماید و در نتیجه این الگو، تصمیم‌گیران راهبردی می‌توانند فهم شفاف‌تر و دقیق‌تری را از مؤلفه‌های بازدارندگی در تأمین امنیت سرمایه-های سایبری داشته باشند. بنابراین به‌طور کلی سؤال اصلی این تحقیق عبارت است از اینکه، ابعاد، مؤلفه و شاخص‌های الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها کدامند؟

از آنجایی که این مقاله، پژوهشی اکتشافی بوده و به‌دنبال تدوین الگو است، بنابراین تدوین فرضیه در آن مطرح نیست. برای رسیدن به الگوی مناسبی از بازدارندگی در فضای سایبر، نیاز است تا عناصر و قواعد این موضوع مرتبط با فضای سایبر شناسایی شود. در این پژوهش مواردی چون ارائه الگوی راهبردی از جهت تعیین ابعاد، مؤلفه و شاخص‌های بازدارندگی در فضای سایبر مبتنی بر نظریه بازی‌ها، به‌کارگیری بازی علامت‌دهی با علامت‌های هنجار و ناهنجار، معرفی متغیرهای تابع بهره بازیگران، ارائه شرایط وقوع بازدارندگی و توصیف چگونگی قرارگیری بازیگران در وضعیت‌های ۱- منازعه ۲- توازن ۳- سلطه بازدارنده ۴- سلطه تهدیدکننده ۵- ضعف متقابل (ضرر متقابل) از جمله نوآوری‌های این پژوهش می‌باشند.

مبانی نظری و تعاریف عملیاتی

دو نظریه بازدارندگی سایبری و نظریه بازی‌ها به‌طور کلان در ارائه مدل مفهومی، محور قرار گرفته‌اند و چارچوب نظری ما را شکل خواهند داد. نظریه بازی‌ها در یک سطح کلان‌تر بازی بازدارندگی سایبری را برای ما ترسیم می‌کند که در درون آن متغیرهای تأثیرگذار (علاوه بر متغیرهای مدنظر نظریه بازی‌ها)، توسط نظریه بازدارندگی سایبری تعیین شده است. در ارائه الگوی بازدارندگی در فضای سایبر مدل‌های مختلفی دخیل هستند که مدل امنیت فضای سایبر و سازوکار اندازه‌گیری مخاطره استاندارد ISO/IEC27001، نظریه بازی‌ها به‌طور خاص بازی پویای علامت‌دهی با اطلاعات ناقص، فرض عقلانیت در بازی و تعادل بیزین نش کامل در محاسبه تعادل مدل‌های بازی از جمله آن‌ها هستند که پایه اولیه الگوی ارائه شده تحقیق می‌باشند.

بازدارندگی در فضای سایبر: نظریه بازدارندگی بعضی از اقدامات متقابل و محرک‌ها را برای پیشگیری پیشنهاد می‌کند. بازدارندگی سایبری می‌تواند به‌عنوان توانمندی سازمان‌ها و مؤسسات

برای انکار، محافظت و اقدام متقابل علیه حملات سایبری تعریف شود (*Liles & Davidson, 2013:4*). بازدارندگی سایبری گزینه‌های توسعه‌یافته و رشدیافته بسیاری از روش‌های بازدارندگی سنتی در عصر هسته‌ای جنگ سرد را ارائه می‌کند. همچنین برای اقدام متقابل سنتی، بازدارندگی سایبری، گزینه‌هایی چون اقدامات قانونی، عدم مشاهده شبکه، قابلیت انعطاف و ارتجاعی بودن و وابستگی متقابل را شامل می‌شود و نیز راهکاری جدید چون عدم آسیب‌پذیری ارائه می‌شود (*Jensen, 2012: 773*).

هدف بازدارندگی جلوگیری از اقدامات خصمانه است، به‌وسیله متقاعد ساختن در ذهن دشمن بالقوه، به‌طوری که وقتی عواقب انفعال را محاسبه می‌کند، مخاطراتِ عمل خصمانه سنگین‌تر از مزایای آن باشد (*Jensen, 2012:779*). بازدارندگی به‌طور سنتی اساساً روی تهدید مهاجم بالقوه با پاسخ تنبیه‌گرایانه، به‌منظور بازداری از وقوع حمله تمرکز دارد. به خاطر شرایط خاص فضای سایبر اتکای صرف به اقدامات تلافی‌جویانه ممکن است برای بازدارندگی در برخی شرایط کافی نباشد؛ بنابراین برای سیاست بازدارندگی سایبری چارچوبی شامل چهار فاکتور ۱- جریمه ۲- بی‌ثمری ۳- وابستگی و ۴- ضد بهره‌وری تعیین شده است (*Taipale, 2010:2*).

بازدارندگی عموماً به‌وسیله تهدید، با ترکیب دو عنصر شکل گرفته است: ۱- تنبیه مهاجم به‌وسیله تحمیل هزینه‌های غیرقابل پذیرش و ۲- جلوگیری از موفقیت حمله مهاجمان (*Kesan & Goodman, 2010: 107*) (*Hayes, 2011:434*) در مقاله خود با عنوان یک نظریه از بازدارندگی سایبری درباره بازدارندگی سایبری می‌نویسد: بازدارندگی سایبری همچون همه دیگر بازدارندگی‌ها، وقتی موفق می‌شود که دشمن دیگر تصمیمی برای تجاوز نداشته باشد. این تصمیم دو محاسبه را در بر می‌گیرد، ۱- چه هزینه‌های تجاوز بر مزایای آن بچربد و ۲- چه مزایای خودداری یا جلوگیری، در فضای سایبر بر هزینه‌های آن غالب باشد.

بازدارندگی را عموماً به‌عنوان تأثیرگذاری یک حریف، چه به‌صورت انکار منافع بالقوه یا تهدید استفاده از اقدام تلافی‌جویانه به‌منظور جلوگیری حریف از انجام عملی که شما قصد ندارید او انجام دهد تعریف می‌کنند (*Moore, 2008: 13*). برای موفقیت بازدارندگی، تهدید باید در سطحی باشد که هزینه‌های اقدام حریف نسبت به منافع حاصل بیشتر باشد و نیز تهدید اعتبار لازم را داشته باشد. بنابراین بازدارنده باید قابلیت‌های خود را نمایش دهد و قصد دارد تا تهدید را پیشگیری کند (*Moore, 2008:14*). به زبان ساده‌تر بازدارندگی یعنی: بازیکن A علاقه دارد تا به‌وسیله X، بازیکن

B را از انجام عمل Z به‌وسیله انکار یا تهدید بازدارد. بین بازدارندگی انکار و بازدارندگی تنبیه تفاوت وجود دارد، به‌طوری‌که در بازدارندگی تنبیه حریف تهدید می‌کند حجم زیادی از صنعت و جمعیت او را تخریب خواهد کرد؛ ولی در بازدارندگی انکار بازدارنده حریف را متقاعد خواهد کرد که او در نبرد به اهدافش نخواهد رسید (*Moore, 2008:19*).

به‌طور کلی بازدارندگی یک حالت ذهنی است. این مفهوم تأثیر یک دولت بر انتخاب‌های دولت دیگر است به‌طوری که انتخاب‌هایش در تضاد با منافع دولت بازدارنده نباشد. از نگاه *DOD* ایده اصلی بازدارندگی «به‌طور قاطعانه تحت تأثیر قرار دادن محاسبات تصمیم‌گیری دشمن به‌منظور جلوگیری دشمن از اقدام علیه منافع حیاتی ایالات‌متحده است». کشور بازدارنده تصمیم می‌گیرد تا اقدام قطعی انجام ندهد، زیرا درک می‌کند یا می‌ترسد که در صورتی که این اقدام را انجام دهد ممکن است پیامدهای غیرقابل‌تحملی را به همراه داشته باشد. ایده تأثیرگذاری بر تصمیم کشورها فرض می‌کند کشورها بازیکنان عاقلانه‌ای هستند که خواستار انتخاب روش، برنامه اقدام و وزن کردن هزینه‌ها و مزایای مبتنی بر هزینه – فایده معقول، می‌باشند (*Beidleman, 2009:16*).

بازدارندگی یک رابطه روانی است و هدف آن شکل دادن تصورات و انتظارات حریف و در نهایت تصمیمات وی درباره شروع یک حمله است. بازدارندگی به تهدید کردن حریف، کسی که فکر حمله در ذهن دارد نیازمند است (*Morgan, 2010:56*).

با توجه به پیشینه تحقیق و فرض عقلانیت مبتنی بر نظریه بازی‌ها، بازدارندگی در فضای سایبر را این‌گونه تعریف خواهیم کرد: اگر تهدیدکننده در محاسبه هزینه- فایده مخاطره‌آفرینی علیه بازدارنده، مخاطره اقدامات بازدارنده را علیه خود بیشتر ببیند، آنگاه تهدیدکننده از اجرایی کردن تهدیدات خود خودداری خواهد کرد.

تهدیدات راهبردی در فضای سایبر: 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.

فناوری‌هایی که برای هدایت و ایجاد به ما قدرت می‌دهد همان فناوری‌ها می‌تواند اختلال و تخریب ایجاد نماید (*DoD, 2011:2*). تهدیدات سایبری، به امنیت ملی آمریکا حتی می‌تواند فراتر از اهداف نظامی‌باشد؛ این تهدیدات می‌تواند همه 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, 2011:4*). تهدیدات راهبردی سایبری تهدید به آرمان‌ها، راهبردهای ملی، اهداف کلان نظام، منافع، دارایی‌ها و سرمایه‌های ملی در فضای سایبر است (ملائی و محمدی: ۱۳۹۲).

جامعه دیجیتالی فرانسه در حال شتاب گرفتن است. 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، جاسوسی، تبلیغات، خرابکاری، بهره‌برداری بیش از حد یا استثمار داده‌های شخصی اعتماد و امنیت دیجیتال ما را تهدید می‌کنند (*Prime_Minister_of_France, 2015: 2*).

نیت‌ها (پول، دانش، قدرت، مزیت‌های عملیاتی و ...) هنوز باقی مانده است، اما امکانات به سرعت رشد یافته است. با وسائلی بسیار محدود، انقلاب اینترنتی جاسوسی، خرابکاری، تروریسم، براندازی، 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 (*CHOD, 2014:5*). در سند (*MOD, 2011:15*) مواردی چون جرائم، جاسوسی، تروریست‌ها، هکتیویست‌ها به‌عنوان تهدیداتی که منافع بریتانیا را در فضای سایبر تحت تأثیر قرار می‌دهند، معرفی شده‌اند.

سرمایه‌ها و زیرساخت‌های سایبری: زیرساخت‌های حیاتی یا بحرانی، سازمان‌ها و مؤسسه‌هایی با اهمیت بالا برای بهره‌گیری عموم هستند، به‌طوری که وارد شدن خسارت یا از بین رفتن آن‌ها باعث ایجاد تنگناهای تأمین پایدار، اختلال قابل‌توجه در امنیت عمومی یا دیگر پیامدهای چشمگیر را به همراه خواهد داشت. در سطح فدرال حوزه‌های ۱- انرژی ۲- فناوری اطلاعات و ارتباطات ۳- انتقال ۴- سلامت ۵- آب ۶- غذا ۷- بخش‌های سرمایه‌گذاری و بیمه، ۸-دولت و ۹- رسانه و فرهنگ شناسایی‌شده‌اند (*federal-ministry-of-the-interior, 2011:15*).

سامانه‌ها و سرمایه‌ها چه به‌صورت فیزیکی و یا مجازی، آن‌قدر برای ایالات‌متحده حیاتی هستند که عجز یا اختلال هرکدام از آن‌ها خسارت ناتوان‌کننده‌ای روی امنیت سایبری، امنیت اقتصاد ملی، ایمنی و سلامت ملی، یا هر ترکیبی از آن‌ها وارد خواهد کرد به این‌گونه سامانه‌ها و

سرمایه‌ها زیرساخت‌های حیاتی می‌گوییم (*National-Institute-of-Standards-and-Technology, 2014:37*). سرمایه‌های سایبری عبارت‌اند از زیرساخت‌ها و اطلاعاتی که در شبکه‌های اطلاعاتی و نیز ساختارهای اداری یک نظام اقتصادی موجود است. علاوه بر موارد یادشده، بخش مهمی از این سرمایه، امنیت و سلامت این شبکه است که از مهم‌ترین زیرمجموعه‌های سرمایه‌های سایبری است (اسکندری، ۱۳۹۳: ۸۴).

زیرساخت حیاتی، سامانه‌ها و دارایی‌هایی که اگر نابود شوند، تأثیرات روی امنیت فیزیکی، امنیت اقتصاد ملی و سلامت و یا ایمنی همگانی خواهد داشت. مراکز حیاتی، مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، سامانه‌های هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری سراسری در کشور گردد (همان: ۱۸).

مخاطرات: لغت‌نامه‌های عمومی، ریسک را امکان وقوع اتفاقی (غیرمنتظره)، زیان یا صدمه تعریف می‌کنند. برخی از لغت‌نامه‌های تخصصی‌تر نیز تغییر در بازدهی مورد انتظار یک سرمایه‌گذاری را ریسک می‌دانند. چه این تغییر بازدهی مثبت باشد یا منفی باید دو ویژگی در یک رویداد نهفته باشد تا آن رویداد را ریسک بنامیم. اول امکان وقوع یک رویداد و دوم آسیب‌پذیری نسبت به آن رویداد است (پورصادق و فرشچی: ۱۳۹۲).

مخاطره سایبری، به احتمال بهره‌برداری یک تهدید سایبری، از یک یا چند آسیب‌پذیری سایبری موجود در یک سرمایه ملی سایبری، به‌منظور نابودی یا تخریب، ایجاد اختلال، دسترسی غیرمجاز، افشای اطلاعات، دستکاری اطلاعات یا ممانعت از خدمات محسوب می‌شود (سازمان پدافند غیرعامل، ۱۳۹۳: ۴). با توجه به استاندارد *NIST SP 800-30*، ریسک معیاری است از این‌که یک موجودیت تا چه حد توسط شرایط یا رویداد بالقوه‌ای در معرض تهدید قرار می‌گیرد و معمولاً تابعی از اثرات نامطلوب ناشی از وقوع شرایط یا رویداد و احتمال وقوع ریسک است. ریسک در مواردی مانند عملیات سازمانی (شامل مأموریت، توابع، شهرت)، دارایی‌های سازمانی، افراد، سازمان‌های دیگر به علت پتانسیل دسترسی، استفاده، انتشار، اختلال، اصلاح یا تخریب غیرمجاز اطلاعات و یا سیستم‌های اطلاعاتی وجود دارد (شورای عالی فناوری، ۱۳۹۶: ۱۴). در این پژوهش مؤلفه‌های اصلی مخاطره را احتمال تهدید، ارزش دارایی و سطح آسیب‌پذیری در نظر گرفته شده است و تأثیرات آن به‌طور مشخص در تابع بهره الگو لحاظ شده است.

اقدامات بازدارنده: یک دولت، راهبرد بازدارنده را برای محافظت از منافعش به‌کار می‌گیرد. برای جلوگیری متخاصمین از حمله به آن منافع، یک دولت بیانیه بازدارندگی برای تهدیدکنندگان تهیه می‌کند، به این صورت که این کار را انجام نده، در غیر این صورت آن اتفاق خواهد افتاد (*Goodman, 2010:105*). اقدامات راهبردی بازدارندگی می‌تواند به‌صورت انکاری و تنبیهی باشد. اقدامات انکاری به وقوع پیوستن حمله را با از بین بردن آسیب‌پذیری‌ها ناممکن می‌سازند؛ مانند مقاوم‌سازی و ایجاد افزونه در دارایی‌های حیاتی و اقدامات تنبیهی، کارهایی هستند که در صورت به وقوع پیوستن حمله، مهاجم از طریق آن‌ها خسارات جبران‌ناپذیری را دریافت خواهد کرد. تحریم‌ها و اقدامات قضائی از این جمله هستند.

اقدامات انکاری در دو بخش جلوگیری و بی‌ثمری هستند. در جلوگیری، اقدامات دفاعی موفقیت حمله را مختل خواهند کرد و در بی‌ثمری، اگر حمله‌ای هم رخ دهد، مهاجم از رسیدن به اهداف مدنظر خود بازخواهد ماند. جلوگیری و بی‌ثمری به‌طور کلی بدین معنی است که درنهایت حمله به شکست می‌انجامد. اقدامات تنبیهی، جنبه آفندی بازدارندگی را دارد. اقدامات تنبیهی از اقدام متقابل (تلافی)، وابستگی و ضد بهره‌وری تشکیل‌شده است. در تلافی بازدارنده در صورت حمله به او حمله‌ای به راه خواهد انداخت که هزینه‌های آن سنگین‌تر از منافع حاصل از حمله برای مهاجم خواهد بود. در وابستگی شرایط به‌گونه‌ای است که مهاجم و بازدارنده هر دو دارای منافع مشترک هستند بنابراین این شرایط به ضرر هر دو طرف خواهد بود. ضد بهره‌وری به اهداف تاکتیکی مهاجم بستگی دارد تا اهداف راهبردی او. به‌عنوان مثال در حملات انتحاری، ایالات‌متحده می‌تواند خانواده مهاجم را در صورت حمله، تنبیه کند. این عمل ممکن است عامل حمله را از عمل خود منصرف سازد اما این کار از نظر اخلاقی می‌تواند برای آمریکا تنفرانگیز باشد. بیانیه بازدارندگی باید معتبر و تضمین‌کننده باشد، بدین معنی که بیانیه باید قابل باور و شدنی باشد تا معتبر تلقی شود و از طرفی در صورتی که حمله‌ای صورت نگرفت تضمین شود که او تنبیه نخواهد شد (*Goodman, 2010:106*). گودمن در نهایت همه این مؤلفه‌ها را شکل‌دهنده راهبرد بازدارندگی مؤثر و قوی معرفی می‌کند: منافع، بیانیه بازدارنده، اقدامات انکاری، اقدامات تنبیهی، اعتبار، تضمین، ترس و محاسبات هزینه- فایده.

راهبرد بازدارندگی سایبری برای آمریکا ضروری است، زیرا ایالات‌متحده، نیروهای نظامی آن و متحدانش به حملات بزرگ علیه شبکه‌های اطلاعاتی آسیب‌پذیر هستند. این چنین راهبردی باید

یک چارچوب یا مدل کلی را برای تهیه اقدامات مناسب جهت پاسخ به تهدیدات، شرایط و اهداف ایالات‌متحده به‌کار بگیرد (*Kugler, 2009*). یک بخش تحلیلی، الزامات کلیدی راهبرد بازدارندگی سایبری را بررسی کرده است، این الزامات شامل سیاست اعلامی، آگاهی موقعیتی، فرماندهی و کنترل، امنیت سایبری پدافندی، طیفی از قابلیت‌های آفندی برای اقدام تلافی‌جویانه، همکاری بین سازمانی، همکاری با متحدان، شرکاء و معیارهای بازدارندگی سایبری است. الزامات و اولویت‌های کلیدی برای رسیدن به ظرفیت‌های مؤثر اجرای یک راهبرد بازدارندگی سایبری شامل موارد زیر است: (*Kugler, 2009:18*) ۱- بیانیه سیاست بازدارندگی استوار و شفاف که مقصود بازداری حملات سایبری را تبیین کند. ۲- آگاهی موقعیتی جهانی که برای طیف کاملی از تهدیدات سایبری بالقوه و شرایطی که ممکن است این تهدیدات از آنجا به وجود آید، سازگار شده باشد. ۳- سامانه‌های فرماندهی و کنترل که پاسخ‌های چندمنطقه‌ای هماهنگ شده و میهنی را به تهدیدات سایبری، مجوزدهی خواهد کرد. ۴- پدافند سایبری مؤثر که از نیروهای نظامی و میهنیِ ایالات‌متحده با یک اولویت بالا برای دفاع از زیرساخت‌های کلیدی محافظت خواهد کرد. ۵- طیف وسیعی از قابلیت‌های آفندی سایبری- متقابل، شامل حملات سایبری و دیگر ابزارها برای اظهار قدرت ایالات‌متحده به منظور اعمال بازدارندگی قبل، حین و بعد بحران، ۶- همکاری و همیاری بین سازمانی توسعه‌یافته با متحدان و شرکاء در اروپا، آسیا و دیگر نقاط، ۷- روش‌ها، معیارها و آزمون‌هایی که می‌تواند به فرآیند برنامه‌ریزی کمک کند.

به روشنی به نظر می‌رسد که راهبرد بازدارندگی ایالات‌متحده بهتر است در متن کلی منافع امنیتی و اقتصادی ملی در نظر گرفته شود. در حال حاضر بیشتر عملیات‌های نظامی، سامانه‌های ایمنی عمومی، کسب‌وکار، سیاست و سبک زندگی در آمریکا، مبتنی بر فضای سایبر پی‌ریزی شده است. دفاع سایبری و بازدارندگی سایبری باید رسماً در راهبردهای اقتصادی و امنیت ملی ایالات‌متحده یکپارچه‌شده باشد (*Elder & Levis, 2010:14*). بازدارندگی، راهبردی ملی برای یکپارچه‌سازی نیروها و قدرت دیپلماسی، اطلاعاتی، نظامی و اقتصادی را نیاز دارد. وزارت دفاع باید راهبردها، برنامه‌ها و عملیات‌های مناسب با ادراکات، ارزش‌ها و منافع متخاصمین مشخص را توسعه دهد (*Lukasik, 2010, p. 108*).

بازدارندگی سایبری راهبردی است که دولت مدافع، به‌وسیله علامت‌دهی اغراض و مقاصدش، برای بازداری از فعالیت‌های خصمانه، نظام تصمیم‌گیری دشمن را هدف قرار می‌دهد و به آن نفوذ

می‌کند و برای جلوگیری از فعالیت‌های سایبری مخرب به‌نوعی متخاصم را از یک تلافی بزرگ‌تر می‌ترساند و به دنبال حفظ وضع موجود (ثبات) است (*Iasiello, 2014:55*). چه در زمان جنگ و چه در زمان صلح یک عنصر کلیدی در بازدارندگی سایبری، توانایی علامت‌دهی نیات به دریافت‌کننده است. بدون توانایی علامت‌دهی، بازدارندگی سایبری به‌وسیله تنبیه بی‌تأثیر خواهد بود و خطر فهم اشتباه و سوءتعبیر به وجود خواهد آمد و خطر تشدید و منازعه را افزایش خواهد داد (*Iasiello, 2014:57*). در مقاله (*Rice et al. 2011:59*) سه راهکار پایه برای بازدارندگی پیشنهاد شده است: ۱- تهدید معتبر یا جلوگیری از مزایا و بهره‌برداری مطلوب دشمن، ۲- تهدید معتبر و تحمیل هزینه‌های جدی به دشمن و ۳- تشویق خویشتن‌داری و متقاعد کردن دشمن که ثبات (عدم اقدام) بهترین گزینه فعلی است.

در نتیجه مطالعه پژوهش‌های گذشته اقدام بازدارنده در سه بعد اقدامات ۱- تنبیهی، ۲- انکاری و ۳- وابستگی دسته‌بندی می‌شوند. در بعد اقدامات تنبیهی مؤلفه‌های ۱- حمله متقابل، ۲- اقدام قانونی، ۳- ضد بهره‌وری، ۴- تحریم‌ها را خواهیم داشت. در بعد اقدامات انکاری یا ممانعتی مؤلفه‌های ۱- انعطاف‌پذیری، ۲- ارتجاعی بودن، ۳- محافظت، ۴- بی‌ثمری، ۵- جلوگیری و ۶- عدم مشاهده را خواهیم داشت و در بعد وابستگی ۱- معاملات تجاری، ۲- پیمان‌ها و ۳- منافع و اهداف مشترک را در قالب مؤلفه‌ها داریم.

علامت‌دهی بازیگران در فضای سایبر: علامت‌دهی می‌تواند به‌صورت آشکار یا مخفیانه یا از طریق کانال‌های دیپلماتیک، اقتصادی یا نظامی اجرا شود. برای مثال در حادثه استاکس‌نت، اگر دولت آمریکا برای استقرار استاکس‌نت روی سانتریفیوژهای ایرانی مسئول بود، دولت آمریکا می‌توانست از طریق کانال‌های دیپلماتیک علامتی برای دولت ایران داشته باشد که اگر ایران فرآیند غنی‌سازی خود را متوقف نسازد، چنین اقدامی بدون اینکه اهداف مدنظر مشخص شود، رخ خواهد داد؛ بنابراین وقتی سانتریفیوژها شکسته و جایگزین شدند، روشن می‌شد که ایالات‌متحده در پشت این حادثه بوده است (*Iasiello, 2014:58*).

مثال دیگر از علامت‌دهی بالقوه در فضای سایبر، می‌تواند استفاده از حملات منع سرویس باشد. در ادامه سناریوی استاکس‌نت، بانک‌های ایالات‌متحده به‌وسیله حملات *DDOS* به صورت کوتاهی بعد از کشف استاکس‌نت مورد هدف قرار می‌گیرند. بسیاری از قانون‌گذاران بلافاصله به دولت ایران که در اجراء و هماهنگ‌سازی حملات از طریق پروکسی‌ها دست داشته است، مظنون

می‌شوند. اگر ایران مسئول بود، پیشتر از طریق علامت‌دهی دیپلماتیک یا شخص سوم بدون آشکارسازی اهداف مشخص، باید به‌طور شفاف به دولت ایالات‌متحده منتقل کند که ایران نه‌تنها در حال پاسخ دادن به استاکس‌نت بود بلکه او ظرفیت‌هایی برای طراحی چنین حملاتی دارد. در مقاله (*Rice et al. 2011:59*) برای علامت‌ها شش خصیصه معرفی می‌کند. این خصوصیات شامل: ۱- روش، ۲- محل، ۳- محدوده، ۴- حساسیت، ۵- اعتبار و ۶- مخفی یا آشکار بودن می‌باشند. در تحقیق (*Hengwei, Jindong, Dingkun, Jihong, & Na, 2015:3*) علامت‌ها متناظر باحالت‌های مدافع در نظر گرفته‌شده است. حالت‌های دفاع در سه سطح ۱- دفاع سطح بالا، ۲- دفاع سطح متوسط و دفاع سطح پائین می‌باشند. علامت‌ها در این مدل نیز در سه دسته علامت دفاع بالا، متوسط و پائین مورد نظر محققین بوده است. در مطالعه (*Pawlick & Zhu, 2015*) مبتنی بر نوع یا حالتی که فرستنده دارد، ارسال علامت انجام می‌پذیرد و محاسبه تعادل بازی بر اساس دسته‌بندی علامت‌دهی تعادل یک‌کاسه و تعادل منفک انجام شده است. در تحقیق (*Zhuang, Bier, & Alagoz, 2010:412*) برای بازی علامت‌دهی چندمرحله‌ای دفاع و حمله، سه نوع علامت صادقانه، مخفیانه و فریبکارانه مورد مطالعه قرار گرفته است.

به‌طور خلاصه علامت‌های مدافع باید دشمن را متقاعد کند که ۱- در رسیدن به اهدافش و حصول مزایایی که به دنبال آن است شکست خواهد خورد، ۲- هزینه‌های جدی متحمل خواهد شد که سنگین‌تر از مزایای در نظر گرفته‌شده است و یا ۳- سبب می‌شود دریافتی‌هایی داشته باشد که به نسبت عدم اقدام، بدتر است و باعث عقب‌نشینی وی می‌شود (*Rice et al. 2011:60*). به‌طور کلی علامت‌ها حاوی اطلاعاتی راجع به نوع بازیکن است؛ بنابراین علامت‌ها ممکن است باورکردنی یا باورنکردنی باشند (سوری، ۱۳۸۶: ۳۱۲). از نگاهی دیگر علامت‌ها می‌توانند به صورت کنترل‌شده با اختیار بازیکن یا کنترل‌نشده بدون اختیار بازیکن باشد. در این تحقیق علامت‌هایی که از سمت تهدیدکننده ظاهر می‌شود، حاوی اطلاعات هستند این علامت‌ها می‌توانند از طریق دسته‌بندی کننده‌های سیستمی یا به صورت خبره‌محور تولید شود.

سامانه‌های آنتی‌ویروس، کشف نفوذ، آگاهی موقعیتی، سرویس دهنده‌های رویدادنگار، مرکز عملیات امنیت، فایروال‌ها و ... از سامانه‌های مهمی هستند که به همراه تحلیل و رصدهای انسانی نقش مهمی در تولید علامت دارند. در این پژوهش علامت‌ها پس از بررسی تحرکات و رفتارهای تهدیدکننده به‌واسطه احصاء ویژگی‌های مشخص از داده‌های جمع‌آوری شده، ترافیک شبکه،

خبرها، اعلام مواضع و ... با تکیه بر تحلیل انسانی و یادگیری ماشین در دو دسته‌بندی هنجار و ناهنجار تهیه می‌شوند. در نهایت یک علامت شرایطی است که در قضیه بیزین با استفاده از آن می‌توان احتمال پسین یا اعتبار تهدید را محاسبه کرد.

تابع بهره در بازی بازدارندگی: با توجه به تعریف عملیاتی بازدارندگی، تابع بهره تابعی بر اساس خسارت‌های ناشی از اقدام حریف، هزینه‌ها و دریافتی حاصل شده از اقدام بازیکن است. خسارت‌ها با محاسبه مخاطره ایجاد شده توسط متغیرهای مرتبط با تهدید، ارزش دارایی و سطح آسیب‌پذیری محاسبه می‌شود. برای تعیین سطح یک آسیب‌پذیری می‌توان از پایگاه داده *CVSS* استفاده کرد (*FIRST, 2017*). هزینه‌ها شامل هزینه‌های علامت‌دهی و اجرای اقدام است و دریافتی حاصل از اقدام، هر نوع عایدی است که در نتیجه اقدام بازیکن به دست می‌آورد. معادله (۱) نحوه محاسبه تابع بهره را برای بازیکنان نشان می‌دهد.

معادله شماره (۱): $U(pl)= E - C – I$

در رابطه شماره (۱) دریافتی بازیکنان با E و هزینه‌ها با C و خسارت‌ها با I نمایش داده شده است.

مدل مفهومی

به‌عنوان مدل مفهومی و در قالب پاسخ به سؤالات تحقیق، الگویی با ابعاد، مؤلفه‌ها و شاخص‌هایی در قالب شکل و جدول شماره (۱) را معرفی خواهیم کرد. دارایی‌ها و تهدیدات سایبری می‌توانند در ابعاد شش‌گانه فناوری، دفاعی- امنیتی، سیاسی، اقتصادی، اجتماعی و حقوقی بر یکدیگر تأثیرگذار باشند و مؤلفه‌های شناخت وضع موجود، وضع مطلوب، تحلیل فاصله و برنامه اقدام به ما کمک خواهند کرد تا بتوانیم در یک فرآیند مشخص، برآورد مناسبی از وضعیت وجود یا حصول بازدارندگی داشته باشیم. شاخص‌های مؤثر بر هر یک از این مؤلفه‌ها در جدول شماره (۱) به همراه تعاریف عملیاتی نشان داده شده است.

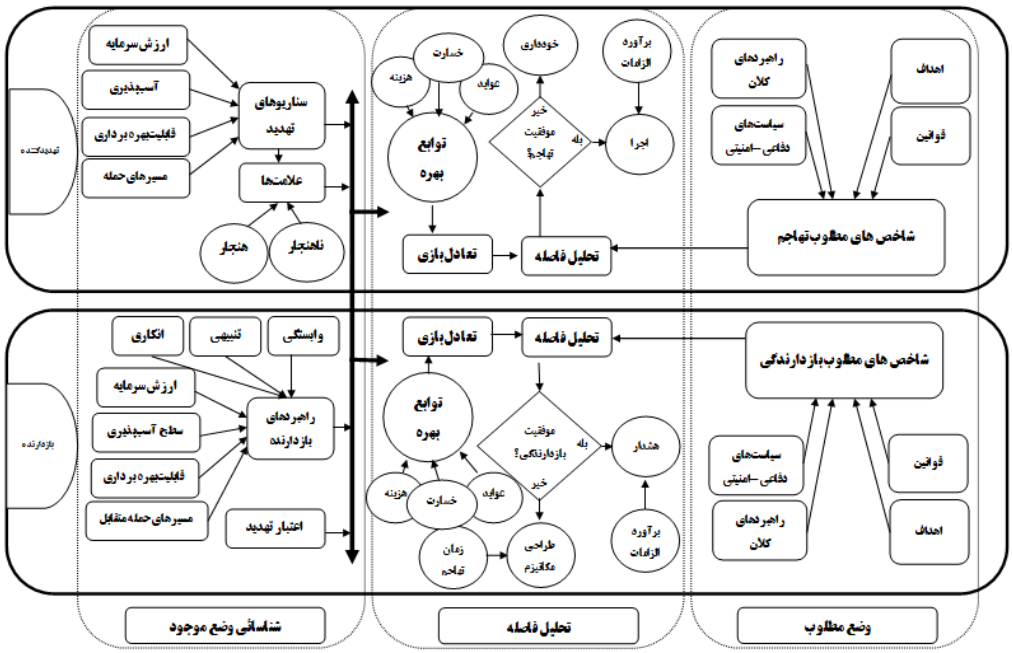
بازدارندگی سایبری به دلیل تعارض منافع در اقدامات بازیکنان نوعی از بازی تلقی می‌شود. در این بازی تهدیدکننده حملاتی را به صورت بالفعل (تهدید) بر علیه بازدارنده در نظر گرفته است که بازدارنده فقط از وجود آن‌ها اطلاع دارد اما از اینکه کدام توسط تهدیدکننده اجرایی می‌شود اطلاعی ندارد و صرفاً علائمی را از سوی تهدیدکننده دریافت می‌کند؛ بنابراین نوعی از بازی علامت‌دهی در بین بازیکنان به وجود می‌آید. تهدیدات برابر مؤلفه‌های بازی علامت‌دهی نوع یا

حالت نامیده می‌شود. هر یک از این حالات دارای احتمال پیشین هستند که در اندازه‌گیری اعتبار تهدید تأثیرگذار است. متناسب با حالاتی که تهدیدکننده دارد علامت‌هایی تولید می‌شود، این علامت‌ها در ساختار بازی علامت‌دهی، راهبردهای فرستنده را تشکیل می‌دهند. در این بازی در گام اول تهدیدکننده متناسب با تهدیدهای (حالت‌ها) خود علامت‌هایی را بروز می‌دهد در گام بعد، بازدارنده اقدامات بازداری کننده خود را خواهد داشت که بر علیه تهدیدکننده در نظر گرفته است. محاسبه نقطه تعادل بازی بر اساس نظریه بیزین نش کامل با توجه به اعتبار تهدید و شکل‌دهی باورها و توابع بهره اندازه‌گیری می‌شود.

بنابراین این بازی از نوع پویا، با اطلاعات ناقص و با سازوکار علامت‌دهی فرض می‌شود. شکل (۱) الگوی بازی بازدارندگی در فضای سایبر را نشان می‌دهد و در جدول شماره (۲) متغیرهای مورد استفاده در معادلات مورد نیاز الگو نمایش داده شده است. هر بازیکن دارایی سایبری مخصوص به خود را دارد. دارایی سایبری ممکن است حداقل یک آسیب‌پذیری یا بیشتر داشته باشد. بازدارنده با توجه به علامت‌هایی که از طرف تهدیدکننده دریافت کرده است و نتیجه محاسبه تعادل بازی، اعلان‌ها و هشدارهای عاقلانه خود را با هدف بازدارندگی اعلام خواهد کرد.

در این تحقیق بازی بازدارندگی در فضای سایبر، به جهت ساده‌سازی و ارائه یک نمونه از کارکرد الگو برای یک آسیب‌پذیری و یک سرمایه سایبری در نظر گرفته شده است. تهدیدکننده در دو حالت حمله (W) یا صلح (P) قرار دارد و بازدارنده در مقابل می‌تواند اقدام (A) یا عدم اقدام (NA) را انتخاب کند. قرار دارند هرچند در محیط واقعی و در شرایط مختلف حالت‌ها، علامت‌ها و اقدام‌های بازدارنده دارای تنوع بیشتری هستند. برای هر حالت تهدیدکننده یک مجموعه دو عضوی از علامت‌ها (σ) وجود دارد. در شروع بازی، تهدیدکننده با توجه به حالت خود، به‌طور خواسته یا ناخواسته علامت‌هایی را در محیط ارسال خواهد کرد، در مقابل بازدارنده با دریافت علامت می‌بایست باوری (μ) را بر اساس علامت ارسال شده از حالت تهدیدکننده محاسبه نماید. این باور اعتبار تهدید را نشان می‌دهد. بازدارنده با توجه به مخاطره ایجاد شده و حالت‌هایی که خود در محیط دارد می‌بایست علامتی را برای تهدیدکننده ارسال کند، این علامت (هشدار و اطلاع‌رسانی) می‌بایست امکان تحمیل مخاطره‌ای را به تهدیدکننده تفهیم کند تا چنانچه تهدیدکننده در حالت حمله (W) قرار داشته باشد از اقدام خود منصرف شود. قضیه بیزین به ما کمک خواهد کرد تا میزان باور یا اعتبار تهدید را محاسبه کنیم. علامت‌های ظاهرشده از سمت تهدیدکننده در

دو نوع رفتار هنجار (N) و ناهنجار (NN) دسته‌بندی می‌شود. با توجه به اینکه راهبردهای بازیکنان با احتمال مشخصی شانس تحقق دارند، بنابراین نوعی از تعادل متأثر از راهبردهای مختلط در بازی وجود دارد این مسئله در بخش تجزیه و تحلیل مورد بررسی قرار خواهد گرفت.



شکل (۱): الگوی بازدارندگی در فضای سایبر در دو ردیف و سه ستون در نمایی فرآیندی نمایش داده شده است. در ردیف بالا گام‌های الگو برای تهدیدکننده و در ردیف دوم گام‌های الگو برای بازدارنده نشان داده شده است. در ستون اول بازیگران وضعیت شاخص‌های وضع موجود خود را محاسبه می‌نمایند و در ستون متغیرهای وضع مطلوب ورودی‌های مورد نیاز برای تحلیل فاصله را فراهم می‌سازد و در ستون دوم با تحلیل فاصله مبتنی بر تعادل بیزین نش، فاصله وضع موجود تا وضع مطلوب و الزامات بازدارندگی مورد ارزیابی قرار می‌گیرد.

بر اساس شاخص‌های معرفی شده در مؤلفه‌های شناخت وضع مطلوب و شناخت وضع موجود داده‌های مورد نیاز برای تحلیل فاصله فراهم خواهد شد. در تحلیل فاصله به‌وسیله محاسبه تعادل بازی موقعیتی که بازیگران در آن نقطه انگیزه تغییر راهبرد را ندارند؛ مشخص خواهد شد. این نقطه یعنی نقطه تعادل، به نوعی پیش‌بینی از آینده را به ما نشان می‌دهد. اما این پیش‌بینی بعد از ممکن بودن دارای احتمال مشخصی است و می‌بایست از جهت تأمین بازدارندگی مورد بررسی قرار گیرد. برابر تعاریف عنوان شده در ادبیات تحقیق، بازدارندگی ارتباط مستقیمی با موازنه و برتری قدرت دارد از این رو بازدارنده بایستی برای تأمین بازدارندگی با تکیه بر حداقل یک برگ

برنده مؤثر، شرایط موازنه قدرت یا برتری قدرت را فراهم نماید. بنابراین اگر در نقطه تعادل حاصل از تحلیل فاصله با توجه متغیرهای تابع بهره (معادله شماره (۱))، بهره هر دو بازیگر صفر یا منفی باشد، این بدان معنی است که ورود در منازعه برای هر دو بهره مثبتی نخواهد داشت و با توجه به فرض عقلانیت بازیگران شرایط بازدارندگی فراهم شده است. در این حالت برابر نیازهای محیط واقعی و وجود عدم قطعیت‌ها، بازدارنده می‌بایست با توجه به نقطه تعادل بازی، هشدار و اطلاع‌رسانی مناسب را برای حصول سطح عقلانیت مناسب اعمال نماید.

هشدارها می‌توانند بیانیه‌ها و اعمالی باشند که از یک ساختار اگر-آنگاه که با توجه به تعادل بازی تعیین می‌شود؛ تولید شوند. به‌عنوان مثال بازدارنده می‌داند اگر تهدید الف عملیاتی شود آنگاه اقدام بازدارنده ب باید اجرا شود بنابراین بایستی با رعایت سطح محرمانگی لازم برای فاش نشدن اهداف اقدام بازدارنده، اعتبار و توانمندی برخورد بازدارنده را به تهدیدکننده تفهیم کند. در صورتی که یک یا هر دو بهره بازیگران در نقطه تعادل مثبت باشد بازی وارد یک منازعه خواهد شد در این وضعیت بازدارنده بایستی با توجه به زمان پیش‌بینی شده از وقوع حمله سازوکار[1] مناسبی را برای تأمین بازدارندگی فراهم نماید.

ابعاد	مؤلفه	شاخص	تعریف عملیاتی
فناوری دفاعی- امنیتی سیاسی اقتصادی	شناخت وضع مطلوب (وضع مطلوب همان آینده مطلوب است. این وضعیت در اسناد بالادستی، سیاست‌ها، راهبردهای کلان و اهداف دولت‌های بازیگران ترسیم شده است.)	اهداف	منظور اهدافی است که در اسناد راهبردی بازدارندگی برای رسیدن به وضع مطلوب تعریف شده‌اند. تحقق این اهداف آمادگی‌های لازم را برای بازدارندگی فراهم می‌سازد.
		راهبردهای کلان	منظور راهبردهای کلان ملی هستند که در ارتباط با بازدارندگی ترسیم شده‌اند و آمادگی‌های لازم برای بازدارندگی را فراهم خواهد ساخت.
		سیاست‌های دفاعی- امنیتی	منظور سیاست‌های دفاعی- امنیتی بازیگران است.
		قوانین	منظور قوانینی هستند که در کشورها مرتبط با بازدارندگی به تصویب رسیده‌اند.
اجتماعی حقوقی	شناخت وضع موجود (منظور شناسایی و اندازه‌گیری ارزش	بازیگران	منظور تعداد بازیگران در بازی است. تهدیدکننده و بازدارنده
		سناریوی تهدید	سناریوی تهدید تعداد مسیرهای حمله به اهداف بازدارنده است که از گراف حمله احصاء می‌شود. مؤلفه‌های اصلی این متغیر مسیر حمله، قابلیت بهره‌برداری، آسیب‌پذیری و ارزش سرمایه و دارایی بازیگران می‌باشد.

1- Mechanisim

	سرمایه‌ها، تهدیدات، آسیب‌پذیری‌های، بهره، باور بازیگران است.)	راهبرد تهدیدکننده	راهبردهای تهدیدکننده همان علامت‌هایی است در محیط بازی از سمت تهدیدکننده بروز می‌کند. علامت‌های هنجار و ناهنجار که بر اساس تحرکات تهدیدکننده ظاهر می‌شود دو نوع علامتی است که در نظر گرفته شده است.
		راهبرد بازدارنده	راهبردهای بازدارنده اقداماتی است که بازدارنده برای ممانعت، تنبیه یا ایجاد وابستگی متقابل برای ایجاد بازدارندگی در نظر گرفته است.
		اعتبار تهدید	باور تهدید همان احتمال یک سناریوی تهدید به شرط مشاهده علامت است و توسط بازدارنده محاسبه می‌شود.
		احتمال راهبرد	منظور شانس اجرایی شدن راهبردهای بازیگران است.
	تحلیل فاصله (منظور از تحلیل فاصله بررسی فاصله بین آینده محتمل و آینده مطلوب است. آینده محتمل به‌وسیله تعادل بازی حاصل می‌شود و آینده مطلوب بر اساس وضعیت مطلوب و شرط بازدارندگی شکل می‌گیرد.)	تابع بهره	در این الگو تحلیل مخاطره بر اساس مؤلفه‌های خسارت، منافع، هزینه و بافت محیط انجام می‌شود. بافت محیط مؤلفه‌ای است که تمایز بین کسب‌وکارها و سازمان‌های مختلف را نشان می‌دهد. تحلیل مخاطره به‌طور مشخص مقادیر اندازه‌گیری شده در تابع بهره بازیگران اعمال می‌گردد.
		محاسبه تعادل	منظور محاسبه تعادل بازی است.
		برآورد الزامات	برآورد الزامات شامل تجهیزات، منابع مالی و زمان انجام اقدام هشداردهی و اطلاع‌رسانی است.
		شرایط بازدارندگی	شرط بازدارندگی معیاری است برای بررسی اینکه آیا شرایط بازدارنده است؟ این شرط در مواقعی برقرار است که هر دو بازیگر همزمان بهره-های کوچک‌تر مساوی صفر داشته باشند.
	برنامه اقدام (برنامه اقدام شامل فرآیندی است که طی آن پیام‌های لازم از سوی بازدارنده برای هشداردهی و اطلاع‌رسانی به تهدیدکننده به منظور بازداری وی ارسال می‌شود.)	هشداردهی و اطلاع‌رسانی	برنامه اقدام مجموعه‌ای از اقدامات است که برای ایجاد بازدارندگی در نظر گرفته می‌شود و هشدار دهی و اطلاع‌رسانی یکی از مؤلفه‌های آن است. منظور از هشداردهی و اطلاع‌رسانی ارسال پیام برای تهدیدکننده به منظور بازدارندگی است.
		طراحی سازوکار	منظور از طراحی سازوکار تعریف شرایط یا بازی جدید در مواقعی است که بازی موجود تعادل آن بازدارنده نخواهد بود.

جدول (۱): ابعاد، مؤلفه و شاخص‌های الگوی بازدارندگی در فضای سایبر

روش پژوهش

نوع و روش تحقیق: این تحقیق از نوع کاربردی- توسعه‌ای بوده و از ترکیبی از روش‌های کمی و کیفی (آمیخته) استفاده شده است. بدین منظور با مطالعه اسناد بالادستی، نظرات اندیشمندان، مصاحبه‌ها و مرور اسناد ادبیات تحقیق، عوامل مؤثر در الگوی تحقیق مورد شناسایی قرار گرفت.

سپس با استفاده از روش کمی (طراحی پرسشنامه)، میزان تأثیر متغیرهای مستقل بر متغیر وابسته بر اساس نظر خبرگان مورد سنجش قرار گرفت. در تهیه پرسشنامه بعد از چند مرحله مصاحبه ارتباط، وضوح و سادگی پرسش‌ها مورد بررسی قرار گرفت و اصلاحات لازم اعمال گردید و همچنین با استفاده از نرخ روایی محتوی[1]ضرورت طرح هر گویه با حداکثر مقدار ۱ و حداقل مقدار ۰,۸ برای هر پرسش حاصل گردید. برای حصول نرخ مناسب پایایی از ضریب آلفای کرونباخ استفاده شد و مقدار ۰,۷۵ برای این ضریب حاصل گردید که نشان دهنده پایایی قابل قبول در داده‌ها است. در ادامه تجزیه و تحلیل یافته‌های پژوهش با رویکرد آماری و ریاضیات نظریه بازی‌ها مورد بررسی قرار خواهد گرفت.

جامعه آماری، روش نمونه‌گیری و جمع‌آوری داده‌ها: به‌منظور دستیابی به ابعاد الگوی راهبردی بازدارندگی در فضای سایبر، ابتدا در پرسشنامه اولیه تعداد ۷۰ سؤال مرتبط با ابعاد، مؤلفه و شاخص‌های الگو در نظر گرفته شد که بعد از تبادل نظرات در خصوص کفایت کاهش سؤالات تحقیق به ۳۸ پرسش، اجماع نظری حاصل شد. پرسشنامه نهایی برای تعداد ۶۵ نفر از جامعه ارسال شد و در نهایت اطلاعات پرسشنامه‌ها توسط ۳۰ نفر از خبرگان آگاه به مسائل دفاعی- امنیتی فضای سایبر در دانشگاه‌ها و مدیریت‌های راهبردی حوزه امنیت فضای سایبر با حداقل میانگین ده سال تجربه، تکمیل و جمع‌آوری شد.

تجزیه و تحلیل یافته‌های پژوهش: بعد از جمع‌آوری داده بر اساس پاسخ‌های داده شده برای هر پرسش میانگین گزینه‌های انتخاب شده در طیف لیکرت پنج گزینه‌ای تأثیرپذیری خیلی زیاد، زیاد، متوسط، کم و خیلی کم محاسبه شده است. متغیرهایی که دارای میانگین تأثیرپذیری بیشتر از ۲,۵ داشته‌اند، به‌عنوان متغیرهای تأثیرپذیر در الگو در نظر گرفته شده‌اند. در جداول (۲) تا (۸) میانگین پاسخ خبرگان به همراه آمار تعداد پاسخ خبرگان به هر یک از سطوح تعیین تأثیرپذیری نمایش داده شده است. ردیف بالاتر در جدول نشان دهنده آن است متغیر از نگاه خبرگان تأثیرگذاری بیشتری داشته است.

ابعاد الگوی بازدارندگی: ابعاد منتخب، توسط نمونه آماری نشان می‌دهد بعد فناوری با میانگین ۴,۵۳ دارای بیشترین اولویت و بعد حقوقی با میانگین ۳,۷ دارای کمترین اولویت تأثیرگذاری از نگاه خبرگان بوده است. در جدول شماره (۲) میزان تأثیر ابعاد و همچنین درصد

1- Content validity ratio

پاسخ‌دهندگان به ازای هر گزینه نمایش داده شده است. تهدیدات تهدیدکننده و اقدامات بازدارنده و نیز، دارایی‌های آن‌ها، می‌توانند در این شش بعد قرار بگیرند، آنچه در این تحقیق تهدیدات، اقدامات و دارایی‌ها را محدود خواهد کرد صرفاً ماهیت فناورانه داشتن و از جنس سایبری بودن مؤلفه‌ها نیست بلکه اثرپذیری و اثرگذاری آن‌ها به‌واسطه ارتباطی که با زیرساخت‌های فناورانه فضای سایبری برقرار می‌کند اهمیت دارد. به‌عنوان مثال یک اقدام بازدارنده در بعد حقوقی در سطح بین‌المللی می‌تواند بازدارنده یک تهدید فناورانه در فضای سایبر باشد.

الگوی	عنوان بعد	میانگین امتیاز تأثیرپذیری	درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
			خیلی‌زیاد	زیاد	متوسط	کم	خیلی‌کم
راهبردی بازدارندگی در فضای سایبر مبتنی بر نظریه بازی‌ها	فناوری	۴،۵۳	۵۳،۳	۴۶،۷	۰	۰	۰
	دفاعی – امنیتی	۴،۴۳	۶۳،۳	۲۳،۳	۱۰	۰	۳،۳۳
	سیاسی	۴،۲۳	۴۳،۳	۴۳،۳	۱۰	۰	۳،۳۳
	اقتصادی	۴،۰۷	۳۰	۵۳،۳	۱۳،۳	۰	۳،۳۳
	اجتماعی	۳،۷	۲۶،۷	۳۳،۳	۲۶،۷	۱۰	۳،۳۳
	حقوقی	۳،۷	۲۲،۲	۳۳،۳	۴۰،۷	۰	۳،۷

جدول (۲): میانگین تأثیرپذیری ابعاد در الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

مؤلفه‌های الگوی بازدارندگی: در جدول (۳) چهار مؤلفه اصلی برای الگوی بازدارندگی توسط خبرگان مورد تأیید قرار گرفته است. مؤلفه »شناخت وضع موجود» با میانگین بیشتر تأثیرگذاری بیشتری را به خود اختصاص داده است و سه مؤلفه دیگر یعنی «برنامه اقدام»، «وضع مطلوب» و «تحلیل فاصله» در سطوح بعدی اولویت ارزیابی خبرگان بوده‌اند.

عنوان مؤلفه	میانگین امتیاز تأثیرپذیری	درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی کم
شناخت وضع موجود	۴،۱	۴۳،۳	۳۳،۳	۱۶،۷	۳،۳۳	۳،۳۳
برنامه اقدام	۴،۰۷	۲۷،۶	۵۱،۷	۲۰،۷	۰	۰
وضع مطلوب	۳،۹	۲۰	۶۰	۱۳،۳	۳،۳۳	۳،۳۳
تحلیل فاصله	۳،۶۷	۱۳،۳	۵۳،۳	۲۳،۳	۶،۶۷	۳،۳۳

جدول (۳): میانگین تأثیرپذیری مؤلفه‌های شناخت وضع موجود، برنامه اقدام، وضع مطلوب و تحلیل فاصله در الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

شناخت وضع مطلوب: در مؤلفه وضع مطلوب شاخص اهداف با میانگین ۴,۷ دارای بیشترین اولویت و شاخص قوانین با میانگین ۴,۰۴ کمترین اولویت تأثیرگذاری از نگاه خبرگان را داشته است.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)		درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی کم
وضع مطلوب (۳,۹)	۱- اهداف (۴,۱۷)	۳۱	۵۸,۶	۶,۹	۳,۴۵	۰
	۲- راهبردهای کلان (۴,۰۴)	۲۹,۲	۴۵,۸	۲۵	۰	۰
	۳- سیاست‌های دفاعی- امنیتی (۳,۹۷)	۲۶,۷	۵۶,۷	۶,۶۷	۶,۶۷	۳,۳۳
	۴- قوانین (۴,۰۴)	۳۳,۳	۴۱,۷	۲۰,۸	۴,۱۷	۰

جدول (۴): میانگین تأثیرپذیری شاخص‌های الگو بر مؤلفه‌های الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

شناخت وضع موجود: در جدول شماره (۵) شاخص‌های گزینش شده برای مؤلفه «شناخت وضع موجود» توسط جامعه خبرگی نمایش داده شده است. در این مؤلفه شاخص بازیگران با میانگین ۳,۹۷ بیشترین اولویت و احتمال راهبرد با میانگین ۳,۷۵ با کمترین اولویت مدنظر خبرگان بوده است.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)		درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی کم
شناخت وضع موجود (۴,۴۱)	۱- بازیگران (۳,۹۷)	۳۹,۷	۳۱	۲۰,۷	۱۰,۳	۰
	۲- سناریوی تهدید (۴,۰۴)	۳۲,۱	۴۲,۹	۲۱,۴	۳,۵۷	۰
	۳- راهبرد تهدیدکننده (۳,۶۴)	۱۷,۹	۳۹,۳	۳۲,۱	۱۰,۷	۰
	۴- راهبرد بازدارنده (۳,۶۴)	۱۷,۹	۳۹,۳	۳۲,۱	۱۰,۷	۰
	۴- اعتبار تهدید (۳,۷)	۲۰	۴۳,۳	۲۳,۳	۱۳,۳	۰
	۶- احتمال راهبرد (۳,۷۵)	۱۶,۷	۵۰	۲۵	۸,۳۳	۰

جدول (۵): میانگین تأثیرپذیری شاخص‌های الگو بر مؤلفه‌های الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

تحلیل فاصله: در مؤلفه تحلیل فاصله، شاخص تابع بهره با میانگین ۳,۹۷ در اولویت اول نظر خبرگان بوده است و شاخص شرایط بازدارندگی با میانگین ۳,۵۷ با کمترین اولویت از نگاه خبرگان نقش‌آفرین بوده است.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)		درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی کم
تحلیل فاصله (۳,۶۷)	۱- تابع بهره (تحلیل مخاطره) (۳,۹۷)	۲۰	۶۰	۱۶,۷	۳,۳۳	۰
	۲- محاسبه تعادل (۳,۸)	۱۰	۶۳,۳	۲۳,۳	۳,۳۳	۰
	۳- برآورد الزامات (۴)	۲۱,۴	۵۷,۱	۲۱,۴	۰	۰
	۴- شرایط بازدارندگی (۳,۵۷)	۷,۱۴	۵۳,۶	۳۲,۱	۳,۵۷	۳,۵۷

جدول (۶): میانگین تأثیرپذیری شاخص‌های الگو بر مؤلفه‌های الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

تابع بهره یکی از مهم‌ترین مؤلفه‌ها در مدل‌سازی و نیز یکی از اجزاء کلیدی در تحلیل فاصله است. همان‌طور که در جدول شماره (۷) نشان داده شده است. از نظر خبرگان شاخص‌های خسارت، هزینه، منافع، هزینه علامت و بافت محیطی به ترتیب در شکل‌دهی تابع بهره تأثیرگذار می‌باشند.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)	عنوان شاخص (میانگین امتیاز تأثیرپذیری)	درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی‌کم
تابع بهره (۳,۹۷)	۱- خسارت (۴,۲۹)	۴۲,۹	۴۲,۹	۱۴,۳	۰	۰
	۲- هزینه (۴,۲۱)	۳۹,۳	۴۶,۴	۱۰,۷	۳,۵۷	۰
	۳- منافع (۴)	۲۵,۹	۵۵,۶	۱۱,۱	۷,۴۱	۰
	۴- هزینه علامت (۳,۶۷)	۱۸,۵	۴۰,۷	۲۹,۶	۱۱,۱	۰
	۵- بافت محیطی (۳,۸۳)	۲۱,۷	۴۷,۸	۲۱,۷	۸,۷	۰

جدول (۷): میانگین تأثیرپذیری شاخص‌های تأثیرگذار بر متغیر سناریو و تابع بهره در الگوی بازدارندگی و درصد پاسخ‌دهندگان به هر یک از سطوح تأثیر

آنچه در این تحقیق از آن با عنوان سناریو نام بردیم وضعیت‌ها یا حالت‌هایی در بازی هستند که از یک سناریوی تهدید حاصل می‌شود. با توجه به نظر خبرگان چهار شاخص اصلی آسیب-پذیری با اولویت اول، ارزش سرمایه یا دارایی با اولویت دوم، احتمال بهره‌برداری با اولویت سوم و مسیر حمله با اولویت چهارم برای تبیین سناریوهای وضعیتی مؤثر هستند.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)	عنوان شاخص (میانگین امتیاز تأثیرپذیری)	درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی‌کم
سناریو (۳,۷۷)	۱- آسیب‌پذیری (۴,۵۷)	۵۶,۷	۴۳,۳	۰	۰	۰
	۲- ارزش (۴,۵۲)	۵۱,۷	۴۸,۳	۰	۰	۰
	۳- احتمال بهره‌برداری (۴,۴۵)	۵۱,۷	۴۱,۴	۶,۹	۰	۰
	۴- مسیر حمله (۴,۰۴)	۲۱,۴	۶۴,۳	۱۰,۷	۳,۵۷	۰

جدول (۸): میانگین تأثیرپذیری شاخص‌های تأثیرگذار بر متغیر سناریو و تابع بهره در الگوی بازدارندگی و درصد پاسخ‌دهندگان به هر یک از سطوح تأثیر

از آنجایی که محاسبه تعادل گام بسیار مهمی در مؤلفه تحلیل فاصله است و می‌بایست از نگاه ریاضیات نظریه بازی‌ها مورد تجزیه و تحلیل قرار گیرد؛ بنابراین در این بخش به تحلیل و فرموله-سازی محاسبه تعادل در بازی بازدارندگی خواهیم پرداخت. گیرنده علامت (بازدارنده pl_2) باید تمام حالت‌های ممکن را که بازیکن فرستنده (تهدیدکننده pl_1) می‌تواند داشته باشد، همراه با احتمال هر حالت (نوع) مدنظر قرار دهد (عبدلی، ۱۳۹۱: ۱۶۳).

در این پژوهش هر نوع یا حالت معادل سناریوی تهدیدی است که توسط هر بازیکن با توجه به مسیر حمله برای حریف در نظر گرفته شده است. بازیکن شروع‌کننده یعنی تهدیدکننده همه انواع خود را به همراه اینکه چه علامتی را ارسال خواهد کرد یا چه علامتی ارسال خواهد شد می‌داند، در مقابل بازیکن بازدارنده حالت یا نوع تهدیدکننده را نمی‌داند، اما اینکه تهدیدکننده چه علامتی را ارسال خواهد کرد؛ می‌داند.

لم (۱): محاسبه تعادل بیزین نشِ کامل در بازی بازدارندگی سایبری سه شرط اساسی را نیاز دارد:

شرط (۱) محاسبه باور است. بازدارنده بعد از دریافت علامت بایستی توزیع احتمال شرطی برای حالت تهدیدکننده را تشکیل دهد.

در شرط (۲) بازیکن بازدارنده بایستی با توجه به باورهای محاسبه‌شده خود و علامت‌های دریافتی، بایستی عمل خود را به‌گونه‌ای انتخاب نماید که بهره انتظاری وی حداکثر شود.

در شرط (۳) قاعده بیزین تعیین‌کننده باورها در بازی است.

اثبات لم (۱): با توجه به اینکه تهدیدکننده دارای حالتی است که توسط طبیعت[1](محیط) برای او مشخص می‌شود و بازدارنده صرفاً اطلاعاتی در مورد احتمال پیشین این حالت دارد، بنابراین برای هر عمل تهدیدکننده باوری را با توجه به قواعد بیزین شکل خواهد داد؛ بنابراین شرط اول تأمین خواهد شد. برای تأمین شرط (۲) بازیکن بازدارنده با تابع شماره (۲) و بازیکن تهدیدکننده با تابع شماره (۳) نقاط تعادلی خود را محاسبه می‌کند.

تابع شماره (۲): $a^*, \lambda^* \in \arg\max_{a,\lambda} U_d[\sigma^*, \mu_l, t_i, \lambda_m]$, $l,i,m=\{1,2\}$

تابع شماره (۳): $\sigma^*, \theta^* \in \arg\max_{\sigma,\theta} U_t[a^*, \theta_n]$, $n=\{1,2\}$

در این توابع U برد انتظاری، a^* راهبرد تعادلی بازدارنده (اقدام A یا عدم اقدام NA)، σ^* راهبرد (علامت) تعادلی تهدیدکننده (علامت هنجار N یا علامت ناهنجار NN)، t_i مجموعه حالات تهدیدکننده شامل جنگ w و صلح p، μ_l باور بازیکن بازدارنده برای هر حالت، λ^* شانس وقوع راهبرد تعادلی بازدارنده، θ^* شانس وقوع راهبرد تعادلی تهدیدکننده را نشان می‌دهند. برای تأمین شرط (۳) با فرمول $\mu(t_i|\sigma_j) = \frac{\mu(\sigma_j|t_i)\mu(t_i)}{\sum_i \mu(\sigma_j|t_i)\mu(t_i)}$ باور بازیکنان مورد محاسبه قرار می‌گیرد. t_i، $i=1,2$ حالت بازیکن حریف را نشان می‌دهد و σ_j، $j=1,2$ نشان دهنده راهبردها یا علامت‌های تهدیدکننده است. با استفاده از سامانه‌های رصد سایبری، احتمال $\mu(\sigma_j|t_i)$ از طریق تاریخچه عملیاتی تهدیدکننده، محاسبه می‌شود.

قضیه (۱): بازی پویای علامت‌دهی با اطلاعات ناقص تهدیدکننده- بازدارنده در الگوی بازدارندگی در فضای سایبر دارای یک تعادل بیزین کامل $(\sigma^*(t_i), a^*(\sigma_j))$ و باور $\mu(t_i|\sigma_j)$ است.

اثبات: با بهره‌گیری از لم (۱) به‌طوری‌که (σ_j^*, a_k^*), $(j,k=\{1,2\})$ مجموعه راهبردهای تعادلی بازیگران و $(\mu(t_i|\sigma_j), \mu(t_r|\sigma_k))$, $(i,r,j,k=\{1,2\})$ نشان‌دهنده باور بازیکنان است. با توجه به اینکه بازدارنده دارای یک حالت در بازی و تهدیدکننده دارای دو حالت جنگ و صلح (خویشتن‌داری) می‌باشد، نیازی به محاسبه $\mu(t_i|a_k)$ برای بازدارنده نیست. می‌توان گفت نمایه راهبردی (σ^*, a^*, μ^*) یک تعادل نش کامل در بازی تهدیدکننده- بازدارنده الگوی بازدارندگی فضای سایبر است. با توجه به اینکه فرستنده به‌طور مشخص برای هر حالت یک علامت ارسال نمی‌کند و این شرایط در محیط واقعی هر علامت با احتمالی مشخص $p(\sigma_j|t_i)$ برای بازدارنده

1- Nature

بروز خواهد کرد. در نتیجه تعادل‌های دیگرِ بازی علامت‌دهی یعنی تعادل‌های منفک[1] یک‌کاسه[2] و نیمه منفک[3] در این الگو به‌کار گرفته نشده‌اند. با توجه به اینکه علامت‌های تهدیدکننده به صورت تصادفی با احتمال θ برای بازدارنده ظهور خواهد کرد و انتخاب راهبردهای بازدارنده نیز برای تهدیدکننده با مقدار λ محتمل است، بنابراین تعادل راهبرد مختلط[4] در بازی وجود خواهد داشت. متناسب با گراف بازی نمایش داده شده در شکل (۲) برد انتظاری بازیکنان با معادلات (۴) و (۵) در جدول شماره (۹) نشان داده شده است.

جدول شماره (۹): برد انتظاری بازیگران متناسب با گراف شکل (۲)

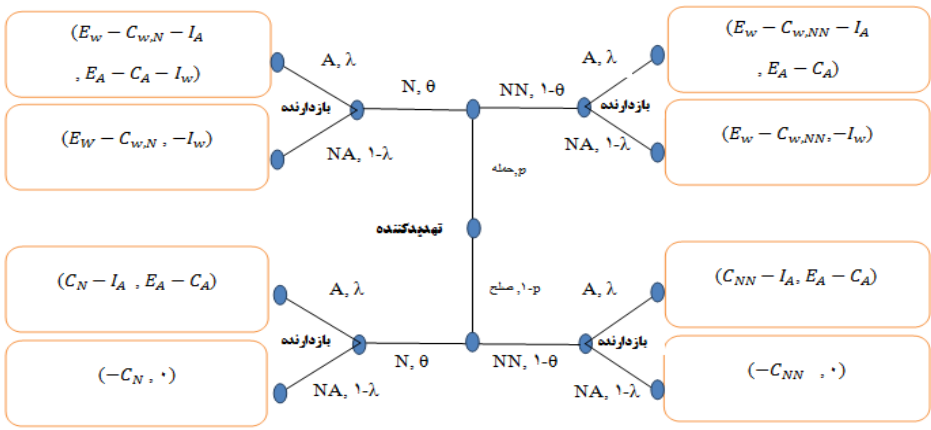
	U_2 معادله (۵) بهره انتظاری بازدارنده	U_1 معادله (۴) بهره انتظاری تهدیدکننده
در حالت حمله (w)	(attack|N) $\theta\lambda(E_A - C_A - I_w)\mu$	$\theta\lambda(E_w - C_{w,N} - I_A)$
	(attack|N) $\theta(1-\lambda)(-I_w)\mu$	$\theta(1-\lambda)(E_W - C_{w,N})$
	(attack|NN) $(1-\theta)\lambda(E_A - C_A)\mu$	$(1-\theta)\lambda(E_w - C_{w,NN} - I_A)$
	(attack|NN) $(1-\theta)(1-\lambda),(-I_w)\mu$	$(1-\theta)(1-\lambda)(E_w - C_{w,NN})$
در حالت صلح (p)	(Peace|N) $\theta\lambda(E_A - C_A)\mu$	$\theta\lambda(C_N - I_A)$
	~~(Peace|N) $\theta(1-\lambda)(0)\mu$~~	$\theta(1-\lambda)(-C_N)$
	(Peace |NN) $(1-\theta)\lambda(E_A - C_A)\mu$	$(1-\theta)\lambda(C_{NN} - I_A)$
	~~(Peace |NN) $(1-\theta)(1-\lambda)(0)\mu$~~	$(1-\theta)(1-\lambda)(-C_{NN})$

در معادلات (۴) و (۵) برد انتظاری برای تهدیدکننده و بازدارنده نشان داده شده است. در این معادلات، E_w دریافتی تهدیدکننده در انجام حمله، E_A دریافتی بازدارنده در نتیجه اقدام متقابل، C_A هزینه اقدام، C_w هزینه حمله تهدیدکننده، C_N و C_{NN} به ترتیب هزینه‌های علامت هنجاری و علامت ناهنجاری و I_w و I_A خسارات حاصل از حمله و اقدام متقابل برای بازیکن حریف را نشان می‌دهد. با توجه به اینکه طبق فرض پژوهش، ظهور علامت‌ها دارای احتمال مشخصی است، بنابراین تهدیدکننده در شرایط با راهبردهای مختلط قرار دارد. در راهبردهای مختلط با مفهومی به نام برد انتظاری یا برد بلندمدت مواجه هستیم (سوری، ۱۳۸۶: ۵۸). بعد از تشکیل توابع برد انتظاری برای بازیکنان، مشتق تابع برد انتظاری بازیکن اول بر اساس احتمال انتخاب عمل بازیکن

1- Separated
2- Pooling
3- Semi-separated
4- Mixed strategy

اول محاسبه می‌شود و نیز در تابع برد انتظاری بازیکن دوم بر اساس احتمال انتخاب عمل بازیکن دوم مشتق‌گیری می‌شود. در ادامه نقاطی که توابع مشتق برابر صفر خواهند شد، احصاء می‌شود. در آن نقاط، نمودار و توابع بهترین پاسخ را می‌سازیم (برای هر دو بازیکن) بنابراین با قرارگیری این دو نمودار نقطه تعادل نش مختلط به دست می‌آید. اگر برای بازیکن اول برد انتظاری عمل بهینه، بزرگ‌تر از برد انتظاری با هر احتمال انتخاب عمل توسط او و احتمال انتخاب بهینه توسط حریفش برقرار باشد، آنگاه می‌گوییم برای هر بازی با N بازیکن که دارای تعداد محدودی از راهبردهای خالص باشد حداقل یک تعادل نش به صورت خالص یا مختلط وجود دارد (سوری، ۱۳۸۶: ۶۳).

در شکل شماره (۲) شکل توسعه‌یافته بازی نشان داده شده است. علامت‌های تهدیدکننده با احتمال $1-\theta$ برای بدرفتاری و احتمال θ برای رفتار نرمال در نظر گرفته شده است و بازدارنده با احتمال λ اقدام بازدارنده را برمی‌گزیند و با احتمال $1-\lambda$ اقدامی نخواهد کرد؛ بنابراین با توجه به ریشه مشتق معادلات U_1 و U_2، (θ^*, λ^*) نشان‌دهنده احتمال بهینه بازیکنان خواهد بود. از این رو در بازی بین بازدارنده و تهدیدکننده که به ترتیب با $pl2$ و $pl1$ نشان داده می‌شوند $((\sigma^*, a^*), (\theta^*, \lambda^*))$ نقطه تعادل در بازی $\Gamma(u_1, u_2, \mu_2, \mu_1)$ الگوی بازدارندگی در فضای سایبر است؛ بنابراین $(\sigma^*(t_i), a^*, \mu(t_i|\sigma_j), \theta^*, \lambda^*)$، بیانگر تعادل کامل بیزین بازی تهدیدکننده-بازدارنده الگوی بازدارندگی در فضای سایبر است.



شکل (۲): گراف بازی پویای بازدارندگی با اطلاعات ناقص. بازیکن اول در حالت جنگ و صلح قرار دارد و در هر حالت می‌تواند با احتمال مشخصی علامت‌های هنجار (N) و ناهنجار (NN) از خود بروز دهد و بازیکن دوم در یک حالت در محیط قرار دارد و می‌تواند در مقابل راهبردهای تهدیدکننده اقدام (A) یا عدم اقدام (NA) را انتخاب نماید.

تعادل حاصل از تحلیل وضع موجود جهت‌گیری بازیکنان در بازی را نشان می‌دهد، اما این به معنی شرایط بهینه برای بازدارندگی نیست. در صورتی که تعادل حاصل، شرایط بازدارندگی را تأمین نماید، آنگاه باید برنامه اقدام تدوین و اجرا شود. یعنی بازیکن بازدارنده بایستی علامتی را تولید و برای تهدیدکننده ارسال کند. در حالتی که تعادل بازی، تأمین‌کننده شرایط بازدارندگی است، اعلام تعادل بازی می‌تواند هشداردهی مناسبی باشد. تهدیدکننده بعد از دریافت اطلاعات هشداردهی درباره مواضع اتخاذ شده توسط بازدارنده، منافع حاصل از اقدام خصمانه خود را در مقایسه با اقدام متقابل بازدارنده کمتر می‌بیند و متقاعد می‌شود تا از اجرایی‌کردن تهدید خود صرف‌نظر کند، چراکه برابر فرض عقلانیتِ بازی، بهره متناسب را دریافت نخواهد کرد. در صورتی که تعادل حاصل شرایط بازدارندگی را برای بازدارنده تأمین ننماید، طراحی سازوکار مرحله دیگری است که می‌بایست در دستور کار بازدارنده قرار گیرد تا بتواند شرایطی را برای تأمین بازدارندگی ایجاد نماید.

برنامه اقدام: بعد از شناخت وضع موجود، وضع مطلوب و تحلیل فاصله، برنامه اقدام در قالب هشداردهی و طراحی سازوکار در دستور کار بازدارنده قرار می‌گیرد. در مؤلفه برنامه اقدام شاخص هشدار و اطلاع‌رسانی با میانگین ۴٫۰۷ با بیشترین اولویت و طراحی سازوکار در اولویت بعدی با میانگین ۳٫۹۶ نقش آن در الگوی بازدارندگی مورد تأیید خبرگان قرار گرفته است.

عنوان مؤلفه (میانگین امتیاز تأثیرپذیری)		درصد پاسخ‌دهندگان به ازای هر سطح تأثیرپذیری				
		خیلی‌زیاد	زیاد	متوسط	کم	خیلی کم
برنامه اقدام (۳٫۹۳)	۱- هشدار و اطلاع‌رسانی (۴٫۰۷)	۳۳٫۳	۴۶٫۷	۱۳٫۳	۶٫۶۷	۰
	۲- طراحی سازوکار (۳٫۹۶)	۱۶	۶۴	۲۰	۰	۰

جدول (۱۰) میانگین تأثیرپذیری شاخص‌های الگو بر مؤلفه‌های الگوی بازدارندگی و درصد پاسخ‌دهندگان به سطوح تأثیر

نتیجه‌گیری

در نتیجه این تحقیق می‌توان عنوان کرد بازدارندگی ارتباط مستقیمی با موازنه قدرت دارد. برای تأمین بازدارندگی در یک وضعیت حداقلی بازدارنده می‌بایست برگ برنده‌ای برای ایجاد موازنه قوا داشته باشد و 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. با توجه به مقادیری که توابع بهره بازیگران به خود اختصاص می‌دهند، پنج وضعیت:

۱- بهره‌های مثبت،

۲- بهره‌های صفر،

۳- بهره مثبت بازدارنده- بهره منفی تهدیدکننده،

۴- بهره منفی بازدارنده- بهره مثبت تهدید کننده،

۵- بهره‌های منفی برای هر دو بازیگر؛

شکل خواهد گرفت. این وضعیت‌ها را به ترتیب وضعیت:

۱- منازعه،

۲- توازن،

۳- سلطه بازدارنده،

۴- سلطه تهدیدکننده،

۵- ضعف متقابل را نام‌گذاری خواهیم کرد.

در وضعیت منازعه ورود به منازعه سایبری برای هر دو بازیگر سودمند است. در وضعیت موازنه ورود به منازعه برای هر دو بازیگر هیچ سودی نخواهد داشت. در وضعیت سلطه فقط برای یکی از بازیگران ورود به منازعه سودمند است. در وضعیت ضرر متقابل هر دو بازیگر از ورود به منازعه متضرر خواهند شد.

در این پژوهش مدل بازی بازدارندگی با اطلاعات ناقص و سازوکار علامت‌دهی در فضای سایبر مبتنی بر تابع بهره مخاطره محور ارائه شد. این الگو وضعیتی را تبیین خواهد کرد که آیا شرایط موجود می‌تواند بازدارندگی ایجاد کند؟ در صورت تأمین بازدارندگی، راهبرد بازدارندگی را ارائه می‌دهد. اقدامات بازدارنده هرچند در دو دسته اقدام و عدم اقدام برای تسهیل در حل مسئله برگزیده شدند؛ اما اقدامات بازدارنده می‌توانند بسته به شرایط بازیگران ذیل دسته‌بندی‌های اقدامات ۱- تنبیهی، ۲- انکاری و ۳- وابستگی متقابل در نظر گرفته شود.

سامانه‌های رصد تهدیدات سایبری و نظارت یکپارچه بر سرمایه‌های سایبری در قالب یک شبکه جامع یکی از نیازهای اساسی کشور است. این شبکه به‌صورت برخط تمامی تحرکات هنجار و ناهنجار دشمن را رصد خواهد کرد و وضعیت بازی را برای سازمان‌های دفاعی و امنیتی کشور تصویر خواهد کرد. برای اجرایی کردن اقدامات بازداری کننده، بازدارنده بایستی به‌طور مداوم

پایش مناسبی از سرمایه‌های سایبری تهدیدکننده داشته باشد و بانک‌های اطلاعی جامع از آسیب-پذیری‌های حریف تشکیل دهد؛ بنابراین برای بهره‌گیری از این آسیب‌پذیری‌ها در مواقع لزوم بازدارنده بایستی زرادخانه‌ای[1]به‌روز از سوءاستفاده‌گرها[2]تدارک ببیند تا بتواند اعتبار لازم را تأمین نماید.

تابع بهره مبتنی بر برآورد مالی فرض شده است، اما این تابع محدوده‌هایی را به وجود می‌آورد. از این رو در شرایطی که ارزش‌های غیرمادی مانند اشتهار یک کشور وجود دارد و امکان کمی-سازی متغیرها وجود ندارد، به‌واسطه نظرسنجی از جامعه و تحلیل انتظارات و ادراکات آن‌ها پارامترهای الگو به‌صورت تلفیقی از مقیاس‌های کمی و کیفی محاسبه خواهد شد.

کارهای آینده: در شرایط مختلف محاسبات پیچیده‌تر خواهد شد و فرموله‌سازی‌ها باید متناسب‌سازی شود این شرایط شامل مواردی چون:

۱- تکرار بازی،
۲- افزایش تعداد بازیکنان و تشکیل ائتلاف،
۳- وجود سیگنال‌های نویزدار،
۴- شدت لحن در علامت‌ها،
۵- صریح و ضمنی بودن علامت‌ها،
۶- تعدد دارایی‌ها و آسیب‌پذیری‌ها،
۷- مدل یادگیرنده بازی،
۸- وجود ارزش‌های غیرمادی

می‌باشند. یکی دیگر از موضوعات پژوهشی که می‌تواند مدل جامع‌تری را از وضعیت بازیکنان و سناریوهای متنوع آن‌ها شکل دهد، طراحی بازی بازدارندگی تهدیدکننده- بازدارنده در فضای سایبر مبتنی بر گراف تهدیدات محتمل، در شبکه سایبری هر بازیکن است.

1- Arsenal
2- Exploit

منابع:

- اسکندری، حمید، (۱۳۹۳)، ***دانستنی‌های پدافند غیرعامل***، دوره عمومی مدیران و کارکنان دستگاه اجرایی، تهران: بوستان حمید.
- پورصادق، ناصر، فرشچی، سیدمحمدرضا و موحدی صفت، محمدرضا، (۱۳۹۲)، ***مدیریت ریسک در محیط‌های نظامی و ارائه یک الگوی ارزیابی مبتنی بر نظریه بازی‌ها***، فصلنامه علمی پژوهشی مدیریت نظامی.
- روشندل، جلیل و طیب، علیرضا، (۱۳۷۳)، ترجمه کتاب ***نظریه بازی‌ها و کاربرد آن در تصمیم‌گیری‌های استراتژیک*** نوشته ونتسل. تهران: نشر قومس.
- سازمان پدافند غیرعامل کشور، (۱۳۹۳)، پایگاه اطلاع‌رسانی پدافند سایبری ایران، سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری کشور، شماره دوم، تیرماه.
- سوری، علی، (۱۳۸۶)، ***نظریه بازی‌ها و کاربردهای اقتصادی***: دانشکده علوم اقتصادی.
- شورای عالی فناوری اطلاعات کشور، (۱۳۹۶)، ***مدل مرجع امنیت***، چارچوب معماری سازمانی ایران.
- عبدلی، قهرمان، (۱۳۹۱)، ***نظریه بازی‌ها و کاربردهای آن (بازی‌های با اطلاعات ناقص، تکاملی و همکارانه)***، تهران: انتشارات سمت، مرکز تحقیق و توسعه علوم انسانی.
- عبدلی، قهرمان، (۱۳۹۲)، ***نظریه بازی‌ها و کاربردهای آن بازی‌های ایستا و پویا با اطلاعات کامل***، تهران: انتشارات جهاد دانشگاهی واحد تهران.
- ملائی، علی و 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.

- Beidleman, Scott W. (2009). Defining and deterring cyber war. Retrieved from
- CHOD. (2014). Belgian Cyber Security Strategy for Defence. ACST–Strategy-CyberSecurity-001 Ed 001 / Rev 000 / 30-09-2014 ACOS STRAT.
- DoD, US. (2011). Department of defense strategy for operating in cyberspace. July. www. defense. gov/news/d cyber. pdf (accessed 14 September 2013.
- Elder, Robert J, & Levis, Alexander H. (2010). Use of Multi-Modeling to Inform Cyber Deterrence Policy and Strategies. Paper presented at the Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy, Washington, DC http://sysarch. gmu. edu/main/media/publications/docs/Elder_NRC_Cyberdeterrence. pdf.
- federal-ministry-of-the-interior. (2011). Cyber Security Strategy for Germany. Alt-Moabit 101 D. 10559 Berlin: Federal Ministry of the Interior. www.bmi.bund.de.

- FIRST. (2017). Retrieved from https://www.first.org/cvss/
- Goodman, Will. (2010). Cyber deterrence: Tougher in theory than in practice? Retrieved from
- Hausken, Kjell, & Zhuang, Jun. (2012). The timing and deterrence of terrorist attacks due to exogenous dynamics. Journal of the Operational Research Society, 63(6).
- Hengwei, Zhang, Jindong, Wang, Dingkun, Yu, Jihong, Han, & Na, Wang. (2015). Defense strategy selection based on signaling game. Paper presented at the Third International Conference on Cyberspace Technology (CCT 2015).
- Iasiello, Emilio. (2014). Is cyber deterrence an illusory course of action? Journal of Strategic Security.
- Jensen, Eric Talbot. (2012). Cyber Deterrence.
- Kesan, Jay P, & Hayes, Carol M. (2011). Mitigative counterstriking: Self-defense and deterrence in cyberspace. Harv. JL & Tech.
- Kugler, Richard L. (2009). Deterrence of cyber attacks. Cyberpower and national security.
- Liles, Jonathan S, & Davidson, Janine. (2013). Modern Cyber Deterrence Theory: Norms, Assumptions and Implications.
- Lukasik, Stephen J. (2010). A framework for thinking about cyber conflict and cyber deterrence with possible declaratory policies for these domains. Paper presented at the Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy.
- MOD, UK. (2011). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world: London: UK MOD.
- Moore, Ryan J. (2008). Prospects for cyber deterrence. Retrieved from
- Morgan, Patrick M. (2010). 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. (2010). Solution architecture for cyber deterrence.
- National-Institute-of-Standards-and-Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity Version ..۱،۰
- Osborne, Martin J. & Rubinstein, Ariel. (1994). A Course in Game Theory: The MIT Press Cambridge, Massachusetts London, England.
- Pawlick, Jeffrey, & Zhu, Quanyan. (2015). Deception by design: evidence-based signaling games for network defense. arXiv preprint arXiv:
- Prime_Minister_of_France. (2015). FRENCH NatioNal digital security strategy. Courtesy translation. Foreword from Manuel Valls, Prime Minister of France, French national digital security strategy.
- Rice, Mason, Butts, Jonathan, & Shenoi, Sujeet. (2011). A signaling framework to deter aggression in cyberspace. International Journal of Critical Infrastructure Protection.
- Schramm, Harrison, Alderson, David L. Carlyle, W. Matthew, & Dimitrov, Nedialko B. (2012). A GAME THEORETIC MODEL OF STRATEGIC CONFLICT IN CYBERSPACE. Paper presented at the In Proceedings of the

۷th International Conference on Information Warfare and Security. Academic Conferences Limited.

- Taipale, KA. (2010 .Cyber-deterrence). Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global.
- Taquechel, Eric F, & Lewis, Ted G. (2012). How to Quantify Deterrence and Reduce Critical Infrastructure Risk.
- Zhuang ,Jun, Bier, Vicki M, & Alagoz, Oguzhan. (2010). Modeling secrecy and deception in a multiple-period attacker–defender signaling game. European Journal of Operational Research.