فصلنامه علمی امنیت ملی
سال سیزدهم، شماره پنجاه، زمستان ۱۴۰۲
مقاله چهارم از صفحات ۱۵۴-۱۲۱

مقاله پژوهشی: الگوی بازدارندگی سایبری از دیدگاه موازین حقوق بین‌الملل

محمدرضا حسینی[۱]

تاریخ دریافت: ۱۴۰۱/۰۸/۲۰ تاریخ پذیرش: ۱۴۰۲/۰۵/۰۹

چکیده

در دورانی که عملیات سایبری افزایش قابل‌توجهی یافته است، بازدارندگی سایبری می‌تواند به عنوان یکی از عوامل مؤثر در ارتقاء امنیت ملی و مقابله با حملات سایبری محسوب شود و در این راستا، توسل به موازین حقوق بین‌الملل و قواعد و مقررات حاکم بر مخاصمات مسلحانه می‌تواند به عنوان عاملی مؤثر در منصرف کردن مهاجم از انجام هرگونه عملیات خصمانه سایبری مورد توجه قرار گیرد. پژوهش حاضر باهدف شناسایی الگوی بازدارندگی سایبری (ابعاد، مؤلفه‌ها و شاخص‌ها و روابط میان آن‌ها) از دیدگاه موازین حقوق بین‌الملل به روش آمیخته، به جمع‌آوری و مطالعه مستندات مرتبط با پرداخته و با کدگذاری و مقوله‌سازی از مفاهیم قابل‌توجه در نرم‌افزار تحلیل کیفی مکس‌کیودا[۲] عوامل قابل‌توجه را احصاء و سپس مدل مفهومی پژوهش را ترسیم نموده است. در ادامه با اخذ نظر خبرگان در خصوص عوامل فوق و تجزیه‌وتحلیل کمی آن‌ها به روش مجذور مربعات جزئی[۳] در نرم‌افزار اسمارت پی.ال.اس[۴]، ضمن اعمال اصلاحات لازم، ابعاد، مؤلفه‌ها و شاخص‌های بازدارندگی سایبری را از منظر موازین حقوق بین‌الملل ارائه نموده است. نتایج پژوهش نشان می‌دهد که از دیدگاه حقوق بین‌الملل، بازدارندگی سایبری را می‌توان در سه بُعد شناسایی (شناسایی عامل تهدید و اخطار زودرس)، هنجارسازی (انتساب مسئولیت و اقدام متقابل یا مقابله‌به‌مثل) و دفاع و تلافی (دفاع مشروع و اقدام تلافی‌جویانه) و مؤلفه‌های چهارگانه (قابلیت، اعتبار، ثبات و ارتباط) و شاخص‌های مربوطه مورد توجه قرار داد.

کلیدواژه‌ها: فضای سایبر، بازدارندگی سایبری، حقوق بین‌الملل، انتساب مسئولیت، اقدام متقابل.

---

[۱] دانشیار حقوق بین الملل و عضو هیات علمی دانشگاه عالی دفاع ملی، تهران، ایران
Rezahsn88@gmail.com

[۲] MaxQDA 2020

[۳] PLS

[۴] SmartPLS

مقدمه و بیان مسئله

امروزه با رشد هر چه بیشتر فضای سایبر و وابستگی‌های زندگی بشری به این حوزه فناوری، تهدیدات سایبری به زیرساخت‌های ملی نیز موردتوجه دشمنان هر جامعه‌ای قرارگرفته است و در کنار آثار مثبتی که در بهبود زیست جهانی دارد، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود و تبعات مخاطره‌آمیز برای بازیگران بین‌المللی دارد که‌آثارش حتی می‌تواند مخرب‌تر از جنگ‌های نظامی بوده و امنیت و حیات ملی دولت‌ها را به چالش بکشاند. از این‌رو، توسعه حملات و عملیات‌های سایبری در زمره مهم‌ترین تهدیداتی محسوب می‌شوند که دولت‌ها و سایر تابعان حقوق بین‌الملل با آن‌ها مواجه می‌باشند. در این راستا، تولید و یا اکتساب تسلیحات سایبری و طراحی الگوریتم‌ها و کدهای رایانه‌ای مخرب و درنتیجه هوشمندسازی تسلیحات و استفاده از «سلاح‌های رباتیک و خودمختار»[1]مهم‌ترین تحول در حوزه درگیری‌های مسلحانه سایبری محسوب می‌شود و در مخاصمات آینده و عرصه پنجم نبرد نقش برجسته‌ای خواهند داشت. تسلیحات سایبری بسیار متفاوت از سایر سلاح‌های سنتی یا حتی سلاح‌های هسته‌ای می‌باشند، چراکه مالکیت بر آن‌ها تنها در اختیار تعداد محدودی از دولت‌ها نیست. برای مثال درحالی‌که سلاح‌های هسته‌ای تنها در اختیار تعداد اندکی از دولت‌هاست، اما اغلب کشورها در تلاش برای ساخت سلاح سایبری می‌باشند و بیش از ۳۰ کشور نیز در نیروهای نظامی خود واحدهای عملیات سایبری ایجاد کرده‌اند. علاوه بر دولت‌ها، سازمان‌های تروریستی و گروه‌های هکری نیز از توانایی انجام اقدامات تهاجمی سایبری مهلک برخوردار می‌باشند (لسانی، ۱۳۹۵: ۹۶).

با توجه به وضعیت آنارشی فضای سایبر، اتکای تنها به راهبردهای امنیتی سنتی «تهاجم-دفاع»، دیگر در مواجه با حملات بالقوه فاجعه‌آمیز سایبری کفایت نمی‌کند و سیاست‌گذاران امنیت ملی باید به راهبردهای دیگری برای مقابله با تهاجمات سایبری فراتر از صرف شناسایی

---

[1] Autonomous weapon systems

و خنثی‌سازی حملات مزبور توجه کنند. صرف دفاع در مقابل خطرات رو به افزایش سایبری که می‌توانند متضمن ایجاد آسیب جدی به زیرساخت‌های حیاتی باشند امری ناممکن است؛ چراکه توانایی عملیات‌های تهاجمی در حال گسترش و دسترسی به تسلیحات سایبری، سهل‌الوصول‌تر شده است. در این راستا، برای مقابله با تهدیدات بالقوه فاجعه‌آمیز حملات سایبری، کارشناسان امنیت ملی اقدام به طراحی و توسعه سازوکارهای بازدارندگی برای تکمیل زنجیره دفاع سایبری خود نموده‌اند. برای مثال، حملات سایبری به زیرساخت‌های حیاتی کشورهای استونی، گرجستان و ج.ا.ایران یادآوری می‌کند که آینده فضای سایبر عاری از حملات و تهدیدات دفاع و امنیتی نخواهد بود و «تئوری بازدارندگی»[1] یکی از موضوعات اساسی هرکشور به‌شمار می‌رود.

مبنای تئوری بازدارندگی شامل مفروضات احتمالی درباره چگونگی تشخیص، تفسیر و واکنش طرف مقابل (دشمن) نسبت به تهدیدات پیش‌رو است. فرض اساسی تئوری این است که تفسیر صحیح یک تهدید از طرف دشمن باعث خواهد شد که وی برخی روش‌ها را به دلیل مخاطره‌آمیز و پرهزینه بودن زیاد را کنار بگذارد. در این زمینه، چالش اساسی این است که ممکن است دشمن احتمالی برداشت و درک درستی از تهدیدات بازدارنده نداشته باشد و برخی حتی ممکن است هیچ احساس تهدیدی نکند و به‌این‌ترتیب، ایجاد بازدارندگی در مقابل آن‌ها سخت‌تر شود. در این پژوهش، مفهوم بازدارندگی به‌صورت کلی متقاعد کردن مهاجم بالقوه به وجود پیامدهای سنگین‌تر در مقابل با منافع حاصل از اقدام سایبری مخرب، به دلیل وجود قابلیت‌های دفاعی در قربانی و یا وجود تهدید معتبر به اقدام تلافی‌جویانه سهمگین توسط قربانی علیه مهاجم، تعریف می‌شود.

در حوزه سایبری و تهدیدات ناشی از حملات و تسلیحات هوشمند، نیازمند شیوه‌های نوین بازدارندگی همچون تلافی، انکار سود حمله و هنجارگرایی می‌باشد. بر این اساس، دولت‌هایی که درصدد توسعه و به‌کارگیری بازدارندگی در فضای سایبری هستند، می‌بایست ملاحظات حقوقی و هنجارهای حاکم را مدنظر داشته باشند، البته ازآنجایی‌که تاکنون اسناد

[1] Deterrence theory

بین‌المللی عام‌شمول و لازم‌الاجرا به‌منظور مقابله با اقدامات خصمانه در فضای سایبری تدوین‌نشده، نحوه مقابله و واکنش در برابر این اقدامات نیز برای دولت‌های قربانی روشن نیست. برای مثال، مسئله انتساب یکی از مهم‌ترین چالش‌های حقوقی است که دولت‌ها در ارتباط با اعمال سازوکارهای بازدارندگی و مقابله با حملات سایبری با آن مواجه هستند. در واقع، انتساب حمله سایبری به عامل واقعی آن، عنصر اصلی در ایجاد یک نظام بازدارندگی مؤثر است چرا که تا زمانی که عامل اصلی تهدیدکننده مشخص نباشد، انتساب مفهوم پیدا نخواهد کرد. همچنین با توجه به ویژگی‌های فضای سایبری، الگوی بازدارندگی در فضای سایبر نیز بسیار متفاوت و دشوارتر از حوزه‌های سنتی خواهد بود. بنابراین، یافتن ابعاد و مولفه‌ها و شاخص‌های اعمال بازدارندگی در فضای سایبری و همچنین چگونگی انتساب اقدامات و حملات سایبری به عامل واقعی آن، مسئله مهمی است که پژوهش حاضر به‌دنبال پاسخ به آن می‌باشد. سوالات اصلی تحقیق برگرفته از مساله پژوهش عبارتند از:

- نسبت به بازدارندگی در محیط سنتی، سازوکار بازدارندگی سایبری از چه ویژگی‌هایی برخوردار است؟
- ابعاد، مولفه‌ها و شاخص‌های اصلی بازدارندگی سایبری کدامند؟
- چه اصول و قواعد حقوق بین‌المللی و حقوق بشردوستانه در ارتباط با بازدارندگی سایبری قابل‌اعمال است؟

با توجه به اکتشافی بودن پژوهش حاضر که در نهایت منجر به ارائه الگوی بازدارندگی خواهد شد و سوال محور است، لذا متغیرهایی مطرح نبوده و در نتیجه فرضیه‌ی (کمی) ارائه نشده و تمرکز پژوهش بر پاسخگویی به سوالات تحقیق که در راستای هدف اصلی تحقیق تدوین گردیده معطوف می‌باشد.

۱. مبانی نظری

با توسعه فناوری‌های سایبری، خطراتی همچون حملات سایبری، تروریسم یا جاسوسی در کمین زیرساخت‌های حیاتی کشورهاست. بازدارندگی سایبری را می‌توان به عنوان بخشی از الگوی دفاع سایبری گنجاند و از این طریق شیوه جامع و نویدبخشی را

برای جلوگیری از وقوع حملات سایبری قبل از این‌که آغاز شوند، به وجود آورد. هدف از بازدارندگی سایبری متقاعد کردن مهاجمان بالقوه به این امر است که آغاز یک تهاجم سایبری به سود اهداف و منافع آنان نخواهد بود و اینکه هزینه‌ها و خطرات اقدام به تهاجم سایبری سنگین‌تر از هرگونه منفعت بالقوه می‌باشد. بازدارندگی در فضای سایبر یک حوزه تعارض بین تهدیدکننده و بازدارنده برای کسب منابع است و باعث می‌شود که تصمیم بازیگران بر یکدیگر تأثیرگذار باشد (عبدلی، ۱۳۹۱: ۲).

الف) مفهوم شناسی

- **تعریف فضای سایبری**: فضای سایبر یک محیط اطلاعاتی است که شامل مجموعه‌ای از زیرساخت‌ها، نرم‌افزارها، شبکه‌های مرتبط به هم شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های کامپیوتری، پردازنده‌ها و کنترلرهای توکار می‌باشد (وزارت دفاع آمریکا، ۲۰۱۱). در تعریفی دیگر این فضا ترکیبی از شبکه‌های ارتباطی، ده‌ها هزار رایانه به‌هم‌پیوسته، سویچ‌ها و کابل‌های فیبرنوری و سرویس‌دهنده‌ها است که امکان ایجاد ارتباطات را فراهم می‌آورد (افتخاری،۱۳۸۲: ۵).
- **جنگ سایبری**: جنگ سایبری به عنوان نوعی نزاع تلقی می‌گردد که در قلمروی دیجیتال یا با استفاده از فضای سایبری رخ می‌دهد، به‌عبارت‌دیگر، جنگ مبتنی بر سایبر به‌نوعی از نزاع تشبیه می‌شود که در پی گسترش فناوری‌های اطلاعاتی امکان‌پذیر شده است (Schneider, 2016: 4-5).
- **تهدیدات سایبری**: هر رویداد یا واقعه باقابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، پنداره یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب) افشاء، تغییر اطلاعات و یا ممانعت (ایجاد اختلال) از ارائه خدمات است (جلالی فراهانی و بیک پوری، ۱۳۹۷: ۱۹٤).

- **بازدارندگی سایبری**: بازدارندگی سایبری یک فرآیند اعم شده است که به معنای مکانیزم منصرف کردن حریف یا دشمن و ممانعت از وقوع درگیری‌ها یا فعالیت‌های تهدیدکننده در فضای سایبری است. فرآیندهای موجود برای بازدارندگی سایبری شامل شناسایی، دفاع، تلافی، انکار سود حمله و هنجارگرایی است (Jasper, 2015 :75).
- **حقوق بین‌الملل**: مجموعه قواعد و مقررات تنظیم کننده روابط بین‌المللی بین تابعان حقوق بین‌الملل است. در واقع مجموعه قواعد حقوقی مرتبط برای کشورها و دیگر سازمان‌های بین‌المللی در روابط متقابل آن‌ها الزام‌آور تلقی می‌شود و منابع حقوق بین‌الملل اساساً بر معاهدات، عرف و هم‌چنین اصول کلی حقوق شناخته شده توسط ملل متمدن پایه‌گذاری شده است (ضیایی بیگدلی، ۱٤۰۲: ۳۵).

ب) پیشینه شناسی

۱) پرویز حسینی و حسین ظریف‌منش در سال ۱۳۹۲در پژوهشی تحت عنوان «مطالعه تطبیقی ساختار دفاع سایبری کشورها» که در دانشگاه جامع امام حسین(ع) منتشرشده است ضمن برشماری ویژگی‌های فضای سایبر و تبیین مفهوم دفاع و حمله در حوزه سایبر، ساختار دفاع سایبری برخی از کشورها را مورد مطالعه قرار داده و ایجاد سازمان دفاع سایبری جمهوری اسلامی ایران را ذیل شورای عالی فضای مجازی، امری ضروری و لازم می‌دانند.

۲) نازنین برادران و همایون حبیبی در مقاله با عنوان «قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری» در مجله مطالعات حقوق عمومی(۱۳۹٦) اعلام می‌دارند تا هنگامی‌که قواعد خاص حقوقی حاکم بر مخاصمات و حملات سایبری موجود نیست، می‌توان در جنگ‌های سایبری قواعد و اصول حقوقی حاکم بر مخاصمات مسلحانه بین‌المللی را اعمال نمود.

۳) احسان اسماعیلی در پژوهشی تحت عنوان «در جستجوی یک نظام حقوقی برای ستیز سایبری» (۱۳۹۳) به مسئله قانونی یا غیرقانونی بودن حملات سایبری و همچنین جایگاه چنین حملاتی در حقوق بین‌الملل با توجه به بند ٤ ماده ۲ و همچنین مواد ۳۹،

۴۱ و ۵۱ منشور سازمان ملل متحد پرداخته است. نگارنده عنوان داشته است که قواعد و مقررات موجود پاسخگوی نیازهای جنگ‌های سایبری نیست و می‌بایست مقررات نوینی به‌منظور اعمال بر جنگ‌های سایبری تدوین گردد.

٤) آمنه بشیری در پژوهشی تحت عنوان حمله سایبری و دفاع مشروع در حقوق بین‌الملل (۱۳۹٤، دانشگاه قم) به موضوع امنیت سایبری را از منظر حقوق توسل به‌زور بررسی کرده است. نویسنده معتقد است که با بررسی حملات سایبری براساس چارچوب‌ها و قواعد موجود حقوق بین‌الملل می‌توان به این نتیجه رسید که میزان زیادی از حملات سایبری انجام‌شده توسط اشخاص، گروه‌ها و دولت‌ها موجب نقض اصل عدم توسل به‌زور، اصل برابری دولت‌ها و همچنین اصل عدم‌مداخله می‌گردد و قربانی چنین حملاتی قادر می‌باشد به دفاع پیش‌دستانه، دفاع مشروع و همچنین اقدامات متقابل متوسل شود.

۵) علی اصغر دهقانی در تحقیقی با عنوان «بازدارندگی سایبری در امنیت نوی جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا که در مجله رهیافت‌های سیاسی و بین‌المللی در سال ۱۳۹٦ به چاپ رسیده، عنوان می‌کند که مقایسه وضعیت کنونی با بازدارندگی جنگ سرد اشتباه است. جلوگیری از آسیب در فضای سایبر، سازوکارهای پیچیدگی‌های مانند تهدید به تلافی، انکار، گرفتار کردن و هنجارها را می‌طلبد.

جمع بندی پیشینه‌ها:

نقاط اشتراک و افتراق پیشینه‌های بررسی‌شده حاکی از این است که اغلب عناوین با یکی از متغیرهای مقاله حاضر وجه اشتراک دارند، به همین خاطر از ادبیات آن‌ها در صورت اقتضاء بهره‌برداری صورت‌گرفته است، اما در هیچ‌کدام از پیشینه‌ها به ارائه الگوی بازدارندگی توجه نشده و بیشتر پژوهش‌ها تنها به بررسی جنبه‌های حقوقی فضای سایبر و نبرد سایبری پرداخته‌اند.

عملیات تهاجمی در فضای سایبری

با گسترش روزافزون دسترسی جهانی به اینترنت و رشد تعداد کاربران نه‌تنها ترافیک جهانی در فضای سایبر افزایش‌یافته، بلکه بازیگران جدیدی در عرصه امنیت سیاسی، اجتماعی، اقتصادی و فرهنگی جهان نمود یافته‌اند که به‌راحتی می‌توانند ماهیت و هویت خود را پشت حکومت‌ها و جنبش‌های اجتماعی مخفی کرده و ضمن طراحی حملات مختلف برای آسیب رساندن به زیرساخت‌های حیاتی یک کشور، زمینه چالش‌های سیاسی و امنیتی را به وجود آورند (زابلی‌زاده و وهاب‌پور، ۱۳۹۷: ٤٨). ازآنجایی‌که فضای سایبر بسیار گسترده‌تر از محیط سیاسی کشورهاست، دولت‌ها نمی‌توانند بر این فضا کنترل کاملی داشته باشند. این مسئله برشدت چالش‌های ایجادشده در چنین فضایی می‌افزاید. این مسئله زمانی که با پیچیدگی‌های عمیق فضای مجازی همراه می‌شود، فضای مناسبی را برای افزایش درگیری‌ها و تضاد در این فضا به وجود می‌آورد.

فضای سایبر محیطی نامتقارن، پیچیده، کم‌هزینه، بدون مرز، در دسترس و غیرقابل‌کنترل است که سهولت انجام عملیات تهاجمی را مقدور ساخته است. این فضا بستری همگانی بوده که انتساب اعمال ارتکابی در این فضا تقریباً غیرممکن است. قابلیت گمنام‌ماندن و ناشناس بودن مهاجم نیز به ویژگی نامتقارن بودن آن افزوده است (Thomasen, 2011: 6). برمبنای این ویژگی‌هاست که پنتاگون درسال ۲۰۰۹ فضای سایبری را به عنوان یک «عرصه جنگی»[1] طبقه‌بندی کرد. درگذشته جنگ مبتنی برحمله و دفاع بود، اما در حال حاضر به علت پیچیدگی فناوری‌های اطلاعاتی و ارتباطی و محیط متغیر و سیال فضای سایبر، مفهوم حمله و دفاع تغییریافته است. به‌گونه‌ای که امروزه دولت‌های مختلف جهان برای تأمین امنیت خود مفهوم دفاع در جنگ‌های سنتی را با الگوهای هوش مصنوعی در فضای سایبر تلفیق کرده و در راستای نظامی‌سازی این فضا گام برداشته‌اند. درواقع

[1] Battlespace

دولت‌های می‌کوشند با تلفیق چهار حوزه درگیری شامل زمین، دریا، هـوا و فـضا با محـیط جدید سایبر، صحنه نبرد را مدیریت نمایند. این رویکرد سبب توجه به تئوری بازدارنـدگی در فـضای سایبری شده است (Goldsmith and Tim Wu, 2006: 29).

بهره‌برداری از ابـزارهای اطلاعاتی بـرای ضربه زدن به دیگران از طریق حملـه مخفیانـه به زیرساخت‌های طرف مقابل، خـرابکاری و اخـتلال در شبکه‌های رایانه‌ای توسط هکرهـا یا بدافزارها که عمدتاً از سـوی توسـط دولـت‌هـا و یـا گـروه‌هـای تروریسـتی تـدارک و پشتیبانی مـی‌شوند انگیزه اصلی حملات سایبری را تشکیل می‌دهند. این حملات می‌توانـد ضربات جبران‌ناپذیری به زیرساخت‌های کشورها وارد کنـد؛ حملاتـی کـه باهـدف از کـار انداختن زیرساخت‌های مهمی چون مخابرات، تأسیسات برق، آب و گاز انجـام مـی‌پـذیرد (لویس و رستملو، ۱۳۹۲: ١٥٤). از سوی دیگر، بازدارندگی یکی از نیازهای اساسی جهـت تـأمین امـنیت ملـی کـشورها اسـت. امـروزه بـا رشـد هرچـه بیشـتر فضـای سـایبر و وابستگی‌های زندگی بشری به این حوزه، تـهدیدات سـایبری به زیرساخت‌هـای ملـی نیـز موردتوجه دولت‌ها و یا گروه‌های تروریستی قرارگرفته اسـت. ازایـن‌رو طراحـی مکـانیزم بازدارنـدگی یکـی از موضوعات اساسی در حـوزه دفـاعی – امـنیتی هـر کشـور اسـت (ملایی و دیگران، ۱۳۹۷: ١٦٧). لذا با توجه بـه اینکـه محـیط سـایبری متفـاوت از قلمـرو فیزیکی است، درنتیجه بازدارندگی در محیط سنتی با محیط سایبری متفاوت خواهد بـود و نیازمند اتخاذ مدل‌های ذهنی جدیدی است. در فضای سایبر عنصر فضا و زمان درهـم‌تنیـده شده‌اند، مهاجمان بالقوه در همسایگی قربانی قرار دارند، تشـخیص هویـت‌هـا و کنشـگران دشوار و اقدامات مبهم می‌باشند. بر ایـن اسـاس، بسـیاری از فـروض زیربنـایی کـه نظریـه بازدارندگی در قلمروی فیزیکی بر آن‌ها استوار هستند، در فضای سایبر بـه چـالش کشـیده شده‌اند و در نتیجه مؤلفـه‌هـای بازدارنـدگی در محـیط فیزیکـی و فضـای سـایبر متفـاوت خواهد بود (Geer, 2007: 17).

الف) بازدارندگی در محیط سنتی

بازدارندگی یک روش پرکاربرد در تاریخ سیاست بین‌الملل و بسیاری از روابط اجتماعی دیگر است و تا قبل از جنگ جهانی دوم تا حد زیادی امری تلقی می‌شد که زیاد مورد توجه قرار نگرفته بود. در اوایل جنگ سرد، تحلیلگران و سیاست‌گذاران شروع به استفاده از آن به عنوان آخرین راه‌حل برای جلوگیری از یک جنگ بزرگ دیگر کردند، که منجر به توسعه اولین تحلیل گسترده نظری بازدارندگی در سیاست بین‌الملل و همچنین مبنای بسیاری از سیاست‌های دفاعی و راهبردهای ملی گردید. در سیاست بین‌الملل، بازدارندگی به تلاش برای جلوگیری از حمله عمدی با استفاده از تهدیدها برای واردکردن آسیب غیرقابل‌قبول به مهاجم، تعریف می‌شود. آسیب‌های موضوع تهدید می‌توانند با یک دفاع مستحکم، بی‌حاصل کردن حمله یا بیش‌ازحد پرهزینه کردن ادامه دادن آن یا تبدیل موفقیت به پیروزی بی‌ارزش، تحمیل شوند (Will, 2010: 127).

در فضای فیزیکی گونه‌های مختلفی از استراتژی‌های بازدارنده وجود دارند که به موفقیت‌های خوبی دست‌یافته‌اند که می‌تواند به عنوان معیارهای بالقوه بازدارندگی سایبری مورد استفاده قرار گیرد. بااین‌حال، هرچند برخی اشتراکات مانند تهدیدهای بالقوه مختلف، توانایی‌های نامتقارن مدافعان و متجاوزان و عملیات نظامی وجود دارد، اما هرکدام چالش‌های منحصربه‌فرد خود رادارند که قابل‌مقایسه نیستند.

۱) بازدارندگی هسته‌ای: هیچ نمونه روشن‌تری از استراتژی بازدارندگی هسته‌ای که در طول جنگ‌سرد اعمال شد، وجود ندارد. بازدارندگی هسته‌ای متوجه کشورهایی بود که قبلاً به سلاح هسته‌ای مجهز شده بودند و هدف این استراتژی جلوگیری از کاربرد آن بود نتیجه بازدارندگی هسته‌ای یک موفقیت قاطع بود، زیرا از پایان جنگ جهانی دوم تاکنون هیچ کشوری تسلیحات هسته‌ای را علیه هدفی مورداستفاده قرار نداده است، زیرا هزینه‌های مربوط به به‌کارگیری آن بسیار بیشتر از مزایای احتمالی آن است (Record, 2004: 14).

۲) بازدارندگی تروریسم: برخی بر این باورند که بازدارندگی تروریسم می‌تواند در برخی از سطوح به موفقیت برسد، به‌ویژه اگر یک سازمان تروریستی از طریق تهدید به آسیب‌زدن به دارایی‌های حیاتی یک کشور، می‌تواند رهبران دولت را وادار سازد تا

سیاست‌های خود را برای حفظ دارایی‌ها مزبور، تغییر یا محدود کنند (Bar, 2008). برای دستیابی به بازدارندگی موفق تروریستی، طرف تهدید شده باید تهدید (ضمنی یا صریح) را درک کند و تصمیم‌گیری توسط دشمن باید به اندازه کافی تحت تأثیر محاسبات هزینه‌ها و منافع باشد. بااین‌وجود، حتی اگر تروریست‌ها به‌طورکلی قابل بازدارندگی نباشند، برخی اقدامات تروریستی قابل بازدارندگی هستند. بااین‌حال، توسل به بازدارندگی تروریسم، در مقایسه با منافع آن با موانع بسیار بیشتری مواجه است (Davis & Jenkins, 2002: 59).

بازدارندگی دولت نافرمان: ایالات‌متحده همواره از راهبرد بازدارندگی در برابر کشورهای نافرمانی که منافع امنیت‌ملی آن را تهدید می‌کنند، بهره‌برده است. کشورهای نافرمان بدون توجه به تلاش‌های ایالات متحده برای متوقف کردن برنامه‌های آن‌ها، همچنان به پیشرفت خود در طرح‌هایی که دولت ایالات متحده آن را خصمانه می‌داند، ادامه می‌دهند. دولت بوش در دوره دوم خود رویکرد جدیدی تحت عنوان «بازدارندگی متناسب»[1] را اعلام کرد که جهت استفاده علیه کشورهای نافرمان طراحی‌شده بود (Knopf, 2013). مبنای این استدلال این بود که می‌توان استراتژی‌های مختلفی را برای کشورها و موقعیت‌های مختلف تدوین کرد (Emilio, 2014: 61).

ب) بازدارندگی در فضای سایبری

امروزه بخش اعظمی از توجهات به محافظت از اطلاعات و فناوری اطلاعاتی معطوف است که برای یک کشور مهم می‌باشند. انجام چنین حفاظتی به دو روش (سازگار با هم) جستجو می‌شود، دفاع از دارایی‌ها در برابر اقدامات خصمانه و منصرف کردن طرف متخاصم از انجام چنین اقداماتی. دفاع شامل اقداماتی است که احتمال موفقیت یک حمله تهاجمی را کاهش می‌دهد. این امر موارد شامل اقداماتی است که مانع از ایجاد دسترسی توسط مرتکب، کاهش آسیب‌پذیری‌ها یا بهبود سریع قربانی پس از انجام یک عملیات تهاجمی موفق می‌باشد. منصرف کردن عبارت است از متقاعد کردن یک دشمن به عدم

[1] Tailored Deterrence

انجام اقدام تهاجمی از ابتدا. بازدارندگی روشی جهت منصرف کردن است که شامل تحمیل هزینه‌های سنگین به هر دشمنی می‌باشد که به‌اندازه کافی عاملی برای عدم شروع یک اقدام تهاجمی نیست (Lynn, 2010).

(۱) عوامل موثر در استراتژی بازدارندگی سایبری

هدف بازدارندگی جلوگیری از اقدامات خصمانه است، به‌وسیله متقاعد ساختن در ذهن دشمن بالقوه به‌طوری‌که وقتی عواقب انفعال را محاسبه می‌کند، مخاطرات 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 استراتژی بازدارندگی سایبری چارچوبی شامل چهار عامل: «جریمه، بی‌ثمری، وابستگی و ضد بهره‌وری» تعیین‌شده است (Taipale, 2010: 311).

(۲) شیوه‌های اعمال بازدارندگی سایبری:

بازدارندگی موفقیت‌آمیز وابسته به تهدیدی است که به‌صورت مکفی اعلام‌شده، معتبر و باورکردنی بوده و به‌آسانی قابل رد نیست. ازآنجایی‌که اعمال بازدارندگی ممکن است از انواع مختلفی از تهدیدات جلوگیری کند، بحث در مورد شرایط بازدارندگی موفقیت‌آمیز تا حد زیادی دشوار است، زیرا این راهبرد نه‌تنها باید با رقیب، بلکه با نوع عملی که مدافع سعی در جلوگیری از آن دارد سازگار باشد. بازدارندگی عموماً از طریق ترکیب دو عنصر شکل می‌گیرد (Hayes & Kesan, 2011: 434):

۱) تنبیه مهاجم به‌وسیله تحمیل هزینه‌های غیرقابل‌پذیرش؛

۲) جلوگیری از موفقیت حمله مهاجمان.

برخی نویسندگان و محققین بر این باورند که بازدارندگی سایبری به دو شیوه دنبال می‌شود: الف) بازدارندگی از طریق انکار سود که از طریق مجازات مهاجم (بازدارندگی فعال) حاصل می‌شود؛ ب) بازدارندگی از طریق تلافی یا توانایی خنثی کردن یک حمله (بازدارندگی غیرفعال) انجام می‌شود (Libicki, 2009: 121).

بنابراین نکته مهم در مورد بازدارندگی سایبری، ایجاد تعادل بین هزینه‌های حمله و احتمال موفقیت پیش‌بینی‌شده است. به‌عبارت‌دیگر، برای برخی از مهاجمان که هزینه‌های اقدام به حمله نزدیک به صفر است، حتی یک شانس موفقیت بسیار کوچک در مقایسه با هزینه حمله، تقریباً به معنای اقدام به حمله خواهد بود. بنابراین، در فضای سایبر دستیابی به احتمال موفقیت نزدیک به صفر به‌سادگی امکان‌پذیر نیست، اما هرچه دولتی نزدیک‌تر به سیستم‌هایی با سطح امنیتی کامل یا تقریباً کامل برسند، احتمال خودداری مهاجمان بالقوه از دست زدن به حمله بیشتر وجود دارد.

(۳) ابعاد بازدارندگی سایبری:

استراتژی بازدارندگی سایبری دارای ٦ بعد اساسی مهم به شرح زیر است:

۱) **شناسایی**: توانمندی مرتبط ساختن حمله‌ای به یک بازیگر یا منبع خاص است که اعتبار و مشروعیت بازیگر را در عرصه داخلی و خارجی حفظ می‌کند. بازدارندگی کامل نیازمند آن است که اولاً تهدیدکننده و یا مهاجم شناسایی شود و ثانیاً به‌طور بالقوه هیچ شانس موفقیتی را برای خود انتظار نداشته باشد.

۲) **دفاع**: طراحی یک سیستم دفاعی مستحکم اولین گام در راه محافظت از منابع و زیرساخت‌های کشورها در برابر اکثر مهاجمان بوده و اغلب آن‌ها را از انجام حمله منصرف می‌سازد. در اینجا، مدافع تا حد زیادی تعیین‌کننده نتایج می‌باشد. هرچند درک و به‌کارگیری یک دفاع قوی نیز ساده‌تر است، اما دفاع می‌تواند بسیار پرهزینه و دشوار باشد، بنابراین بازدارندگی مؤثر ارجح بر دفاع فعال می‌باشد، چراکه امنیت با هزینه کمتر و بدون ضرر حاصل می‌شود.

۳) **تلافی**: تمایل و توانمندی تلافی علیه هر حمله‌ای از هر منبعی و تحت هر شرایطی باید ایجاد شود. اما به دلیل عدم قطعیت امکان شناسایی حمله‌کننده، تهدید به‌تلافی کارایی زیادی ندارد. با این‌وجود، این سازوکار هم چنان به عنوان یکی از مهم‌ترین بخش‌های معادله بازدارندگی در فضای سایبر باقی خواهد ماند و پاسخ‌های تلافی‌جویانه متناسب با شدت حمله خواهد بود. تهدید به اقدام به تلافی‌جویانه، اگرچه ممکن است همه دشمنان بالقوه را کاملاً منصرف ننماید، اما بسیاری از دشمنان را از انجام حمله باز می‌دارد. این امر در مورد بازدارندگی سایبری نیز صادق است. به‌صورت کلی، شرایطی لازمی که تحت آن راهبرد بازدارندگی از طریق اقدامات تلافی‌جویانه موفقیت‌آمیز خواهد بود عبارت‌اند از:

الف) تهدید جدی و مهم؛

ب) بیان صریح رفتارهای چالش‌برانگیز و واکنش تهدیدآمیز؛

پ) اعتبار (باورکردنی بودن) واکنش؛

ت) مسلم بودن مجازات (Morgan,2010: 56).

٤) **انکار**: استفاده از مکانیزم انکار بیشتر می‌تواند گروه‌ها و دولت‌های ضعیف را از حمله منصرف کند و دولت‌های قوی دارای آن‌چنان قدرت بالایی هستند که با استفاده از انکار قادر به بازداشتن طرف مقابل از حمله شوند. زمان‌بر بودن فرایند انتساب حمله سایبری به عامل واقعی آن به این معناست که تهدید به تلافی‌جویی به‌تنهایی نمی‌تواند مهاجمی را از انجام یک حمله سایبری سهمگین منصرف کند، خصوصاً اگر مهاجم چیز زیادی برای از دست دادن نداشته باشد یا در خصوص مهارت‌های حمله سایبری خود مطمئن باشد. بازدارندگی سایبری از طریق اقدام به تلافی‌جویی به‌تنهایی کافی نیست، لذا با توسل به انکار، متجاوز متقاعد می‌شود که حملات سایبری علیه قربانی قادر به دستیابی به اثرات مطلوب وی نخواهد بود یا کاملاً شکست خواهد خورد (ملایی و دیگران، ۱۳۹۷: ۱٤۳).

۵) **گرفتارسازی:** استفاده از این سازوکار مستلزم درک مشترک همگان مبنی بر سودمندی استفاده از فضای مجازی برای مهاجم و مدافع است. در صورت رسیدن به چنین درکی، قطعاً هیچ بازیگری به‌دنبال استفاده غیر صلح‌آمیز از این فضا نخواهند بود. در واقع این سازوکار براساس وابستگی متقابل کار می‌کند. برخی از وابستگی‌ها دو یا چند طرفه هستند. در این حالت کشورها به دنبال ثبات سیستم خواهند رفت. البته این سازوکار برای همه کشورها کارایی ندارد؛ به عنوان مثال کشوری مانند کره شمالی را نمی‌توان با این مکانیزم از انجام حملات و یا تهدیدات سایبری منصرف نمود (فریدمن، ۱۳۸٦: ۵۵).

٦) **هنجار:** آخرین سازوکار، هنجارها و تابوها هستند. مسئله شناسایی در عملکرد این سازوکار نیز اهمیت پیدا می‌کند. درصورتی‌که بتوان با تصویب قوانین بین‌المللی، عملیات سایبری را به‌صورت تابو و هنجار الزام‌آور درآورد، آنگاه شکستن تابو برای کشورها هزینه خواهد داشت. بازدارندگی از این طریق، قدرت نرم کشورها را هدف قرار می‌دهد. هنجارها باگذشت زمان شکل می‌گیرند و هنجارسازی مراحلی دارد که در حوزه سایبری، در مراحل اولیه آن قرار داریم (رمضان‌زاده و دیگران، ۱۳۹۹: ۷۹).

(٤) مؤلفه‌های بازدارندگی سایبری

یک نظام بازدارندگی مؤثر صرفاً به داشتن نیروی نظامی قدرتمند متکی نیست، بلکه یک قدرت بازدارنده مؤثر علاوه بر داشتن امکانات و سازوبرگ نظامی، مؤلفه‌های دیگری باید داشته باشد که عبارتند از:

الف) قابلیت: این مؤلفه به توانایی دولت‌ها در انجام بازدارندگی می‌پردازد؛ یعنی توانایی وارد آوردن ضربه به مهاجم احتمالی به‌وسیله تجهیزات متعارف و غیرمتعارف. نیروی بازدارنده باید قادر باشد در صورت لزوم مجازات متناسب را برای طرف مهاجم به مرحلهٔ عمل درآورد.

ب) اعتبار: یعنی قبول داشتن و اعتماد به توانمندی خود و اراده لازم برای بازداشتن مهاجم از تهاجم؛ به عبارتی بازدارندگی زمانی مؤثر است که توانایی کافی برای پاسخ به تهدید، وجود داشته باشد.

ج) ثبات: طرف‌های منازعه نه‌تنها باید بتوانند تصمیم به اجرای تهدید را به یکدیگر بفهمانند، بلکه باید رهبران دشمن را در مورد نیت خود تحت تأثیر قرار دهند؛ بازدارندگی مؤثر علاوه بر معتبر بودن، باید باثبات هم باشد.

د) ارتباط: در نظریه بازدارندگی، جلوگیری از برخورد میان طرفین، به تبادل‌نظر صریح و ضمنی طرفین بستگی دارد. بنابراین آن چیزی که بازدارندگی سایبری را از نوع سنتی آن متمایز می‌کند، تفاوت در نوع، شیوه‌ها، مکانیزم‌ها و منبع حمله است (رمضان‌زاده و دیگران، ۱۳۹۹: ۷٤).

بازدارندگی سایبری و حقوق بشردوستانه بین‌المللی

اسناد حقوق بین‌الملل به‌صراحت به انجام فعالیت‌های سایبری خصمانه‌ای که از فراتر از مرزهای ملی اتفاق می‌افتد، نپرداخته است. بااین‌حال، «کنوانسیون جرائم سایبری»[۱] تلاش نموده تا برخی از اقدامات و فعالیت‌های خاص مربوط به رایانه را جرم‌انگاری کند و همکاری بین‌المللی در انجام تحقیقات را توسعه دهد. همچنین، «کنوانسیون بین‌المللی مخابرات»[۲]، دولت‌های عضو را از دخالت مضر در ارتباطات از راه دور منع کرده و «موافقت‌نامه جلوگیری از فعالیت‌های خطرناک نظامی»[۳]، ایجاد اختلال مضر در سیستم‌های فرماندهی و کنترل معارضان نظامی را منع می‌کند. با این‌وجود، در خصوص حملات سایبری، نظام حقوق بین‌الملل موجود فاقد مقررات روشن و شفاف است. در این وضعیت، بسیاری از حقوقدانان معتقدند که باید مطابق با مقررات حاکم بر مخاصمات مسلحانه

---

[۱] The Convention on Cybercrime of the Council of Europe was opened for signature in Budapest in November 2001.

[۲] International Telecommunication Convention

[۳] Agreement on the Prevention of Dangerous Military Activities

بین‌المللی و منشور ملل متحد رفتار شود (Hayes & Kesan, 2011, 451). حمله سایبری، نوعی حمله است که در آن از طریق رایانه‌ها و شبکه‌ها سیستم‌های هدف را غیرقابل استفاده نموده، کارایی آن را کم کرده، و با ورود اطلاعات غلط دقت تصمیم‌گیری کاربران را کاهش می‌دهد. حملات سایبری چند تفاوت عمده با شکل‌های معمول حمله دارند:

۱) حملات سایبری توسط عوامل ناشناس صورت می‌گیرد و ردیابی و یافتن محل اختفای آن‌ها بسیار دشوار است.

۲) حمله سایبری، عنصر زمان و مکان را محو کرده و از بین می‌برند.

۳) حمله‌های سایبری بسیار ارزان‌تر و فاقد آسیب‌پذیری و هزینه هستند.

٤) به دلیل ماهیت ساختارهای شبکه اشخاصی که اقدام به انجام حملات سایبری می‌نماید، اشخاص مزبور در برابر هرگونه مقابله‌به‌مثل و تلافی‌جویی محافظت می‌شوند (اسماعیلی، ۱۳۹۳: ۲۵).

نکته مهمی که می‌بایست در موردحمله سایبری موردتوجه قرار گیرد اینکه عموماً از رویکردهای فنی یکسانی برای نفوذ در امنیت یک سیستم یا شبکه استفاده می‌شود. عملیات تهاجمی سایبری، می‌تواند دربردارنده هر دو مرحله تهدید و حمله باشد (Lin, 2011: 131). به‌تازگی تسلیحات سایبری به زرادخانه‌های تسلیحاتی سنتی اضافه‌شده‌اند که دولت‌ها و دیگر گروه‌ها می‌توانند هنگام درگیری با یکدیگر از آن‌ها استفاده نمایند. بنابراین، در دسترس بودن تسلیحات سایبری برای استفاده توسط دولت‌ها، مسائلی را در مورد مشروعیت قانونی و اخلاقی استفاده از چنین سلاح‌هایی ایجاد می‌کند که خود نیازمند تفسیر مجدد از مقررات و قواعد موجود یا ایجاد نظام حقوقی جدید می‌باشد. اکثریت صاحب‌نظران بر این عقیده هستند که اگرچه تسلیحات سایبری متضمن برخی چالش‌های جدید هستند، اما اصول اساسی موجود در رژیم‌های قانونی و اخلاقی موجود همچنان معتبر و قابل اعمال بر نحوه به‌کارگیری آن‌ها هستند.

حقوق بشردوستانه بین‌المللی بیشتر جنبه‌های مربوط به مخاصمات مسلحانه و درگیری‌های نظامی بین‌المللی را موردتوجه قرار داده است. امروز قواعد حاکم بر

مخاصمات مسلحانه در اسناد حقوقی مختلف یعنی منشور سازمان ملل متحد و کنوانسیون‌های ژنو و لاهه بیان‌شده است. اگرچه اصول اساسی حاکم بر صحنه‌های نبرد همچنان معتبر است، اما نحوه اعمال این اصول در درگیری‌های سایبری، نامشخص می‌باشد. کنوانسیون‌های ژنو و لاهه نیز نحوه رفتار دولتی که درگیر مخاصمه مسلحانه است را مقرر می‌کند. گرچه این کنوانسیون‌ها اصول مهمی در خصوص نحوه رفتار دولت‌ها در مخاصمات مسلحانه بین‌المللی را شامل می‌شوند، اما همانند منشور ملل متحد، کنوانسیون‌های مزبور نیز در موردحمله سایبری به عنوان یک شیوه مخاصمه سکوت کرده‌اند و نحوه اعمال اصول ذکرشده در آن‌ها در مخاصمات سایبری روشن نیست. با توجه به اینکه هدف مشروع در مخاصمه تضعیف و کاستن از توان رزمی طرف مقابل است و نه نابودی آن، حقوق مخاصمات مسلحانه محدودیت‌هایی درباره ابزارها و شیوه‌های جنگی مقرر کرده است و هرگونه اقدامی که از هدف مشروع فراتر رود را قبول نمی‌کند.

درمجموع، شیوه‌ها، ابزارها و عملیات سایبری از قواعد حقوق بشردوستانه مستثنا نیستند و هرگاه در حملات سایبری اصول بنیادین حقوق مخاصمات مانند اصل تفکیک، تناسب و ضرورت رعایت نشود، عمل تخلف‌آمیز انجام شده، مسئولیت بین‌المللی دولتها را به دنبال خواهد داشت. برای مثال، استفاده از ابزارها و شیوه‌هایی که به درد و رنج نیروهای متخاصم بینجامد مورد منع این مجموعه حقوقی قرارگرفته است.[1]به عنوان یک اصل کلی و بنیادین حقوق بشردوستانه، افراد و اموال غیرنظامی از حملات و خطرهای ناشی از عملیات نظامی مصون هستند.[2]تأسیسات زیربنایی کشور اعم از آنکه دولتی باشند یا غیردولتی به دلیل کار ویژه و دخالت مؤثر آنها در ملزومات زیست اجتماعی مشمول حمایت‌اند و از حمله مصون شناخته شده‌اند.

ملاحظات حقوقی در زمینه بازدارندگی سایبری:

---

[1] بند «۲»ماده (۳۵)پروتکل اول الحاقی به کنوانسیون‌های ژنو

[2] مواد (۵۱و۵۲) پروتکل اول الحاقی به کنوانسیون ژنو

از منظر حقوقی فرآیند شناسایی مهاجم و یا عامل تهدید، انتساب عملیات سایبری به عامل تهدید و مکانیزم دفاع در تئوری بازدارندگی از اهمیت بالایی برخوردار است. در ادامه این فرآیند مورد بررسی قرار می‌گیرد:

۱) **انکارپذیری هویت و شناسایی عامل تهدیدکننده:** تعداد زیاد کاربران و گمنام ماندن عامل تهدیدکننده در فضای سایبر، موضوع انتقال ادراک خطر به‌مراتب دشوارتر از بازدارندگی سنتی است. عامل تهدیدکننده قادر است که اقدامات خود را از تحت فعالیت‌های کاربران خصوصی یا گروه‌های مختلف پوشش دهد. آنان همچنین می‌توانند با نفوذ در رایانه‌های آسیب‌پذیر و هدایت حملات خود از طریق آن‌ها، هویت خود را مخفی نگه‌دارند. بنابراین، انگیزه و قصد اغلب از طریق روش حمله یا نوع سلاح بکار گرفته توسط عامل تهدیدکننده قابل استنباط یا درک نمی‌باشند و معمولاً قابل‌تشخیص نیست.

۲) **انتساب مسئولیت:** انتساب و مسئولیت‌پذیری در دنیای فیزیکی به‌طورکلی معتبر و ازنظر اثبات پذیری سهل‌تر هستند. قابلیت‌های پاسخ‌گویی را نیز می‌توان از طریق تمرینات و رزمایش‌ها قابل‌مشاهده نشان داد. انتساب فرآیندی است که تعیین می‌کند چه کسی حمله خاصی را انجام داده است. با این‌حال، در قلمروی سایبری، انتساب و مسئولیت‌پذیری قابل‌انکار و رد کردن است. ازآنجایی‌که فعالیت سایبری اغلب ناشناس و مبهم است، انتساب یک حملات سایبری به شخص یا گروه خاصی اصولاً امکان-پذیر نیست. انتساب می‌تواند به‌اندازه تعیین موقعیت جغرافیایی مهاجمان، گسترده؛ و یا خاص‌تر و معطوف به تعیین هویت فردی مهاجمان باشد. انتساب تعیین کننده این است که مالک رایانه، مکان فیزیکی رایانه یا افراد خاصی که مسئول کار با رایانه مهاجم هستند کیست. در صورت انتساب این اقدامات به دولت، طرح مسئولیت بین‌المللی دولت امکان‌پذیر خواهد بود. درصورتی‌که این حملات توسط افراد خصوصی که در استخدام دولت یا تحت کنترل دولت باشند به دولت منتسب می‌شود (Wirtz & Harknett, 2000: 198).

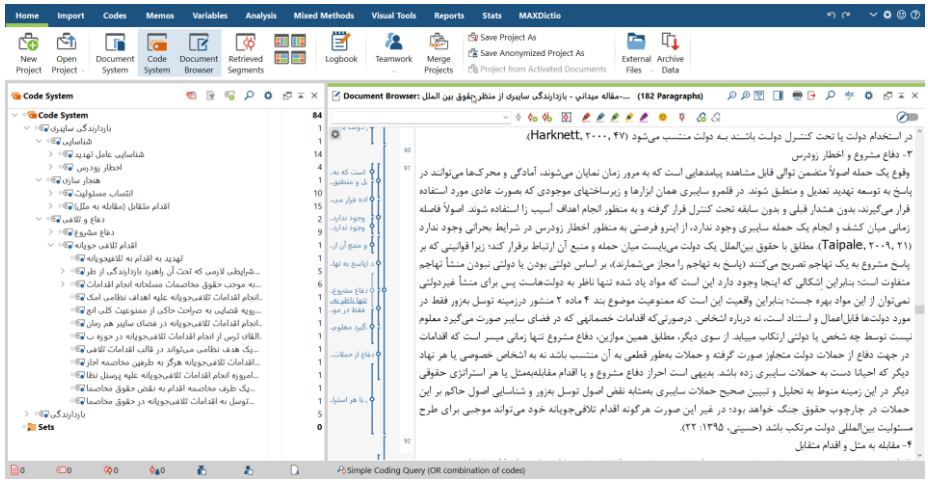
۳) **دفاع مشروع و اخطار زودرس**: وقوع یک حمله اصولاً متضمن توالی قابل‌مشاهده پیامدهایی است که به مرورزمان نمایان می‌شوند، آمادگی و محرک‌ها می‌توانند در پاسخ به توسعه تهدید تعدیل و منطبق شوند. در قلمرو سایبری همان ابزارها و زیرساخت‌های موجودی که به‌صورت عادی مورداستفاده قرار می‌گیرند، بدون هشدار قبلی و بدون سابقه تحت کنترل قرارگرفته و به‌منظور انجام اهداف آسیب‌زا استفاده شوند. اصولاً فاصله زمانی میان کشف و انجام یک حمله سایبری وجود ندارد، ازاین‌رو فرصتی به‌منظور اخطار زودرس در شرایط بحرانی وجود ندارد (Taipale, 2010: 314). مطابق با حقوق بین‌الملل یک دولت می‌بایست میان حمله و عامل آن ارتباط برقرار کند؛ زیرا قوانینی که بر پاسخ مشروع به یک تهاجم تصریح می‌کنند (پاسخ به تهاجم را مجاز می‌شمارند). از سوی دیگر، مطابق همین موازین، دفاع مشروع تنها زمانی میسر است که اقدامات در جهت دفاع از حملات دولت متجاوز صورت گرفته و حملات به‌طور قطعی به آن منتسب باشد نه به اشخاص خصوصی یا هر نهاد دیگر که احیاناً دست به حملات سایبری زده باشد. بدیهی است احراز دفاع مشروع و یا اقدام مقابله به‌مثل یا هر استراتژی حقوقی دیگر در این زمینه منوط به تحلیل و تبیین صحیح حملات سایبری به‌مثابه نقض اصول توسل به‌زور و شناسایی اصول حاکم بر این حملات در چارچوب حقوق جنگ خواهد بود؛ در غیر این صورت هرگونه اقدام تلافی‌جویانه خود می‌تواند موجبی برای طرح مسئولیت بین‌المللی دولت مرتکب باشد (حسینی،۱۳۹۰: ۲۲).

٤) **مقابله‌به‌مثل و اقدام متقابل**: اقدامات متقابل جزء مهم‌ترین مباحث مطرح‌شده در رابطه با مسئولیت بین‌المللی دولت‌ها است که مواد ٤۹ تا ۵۳ از پیش‌نویس مسئولیت بین‌المللی ناشی از رفتار متخلفانه دولت‌ها (مصوب سال ۲۰۰۱ کمیسیون حقوق بین‌الملل) را به خود اختصاص داده است. کمیسیون حقوق بین‌الملل طی مواد مذکور به هدف، محدوده، شرایط و سایر مسائل مربوط به اقدامات متقابل پرداخته است. هدف اقدام متقابل، حمایت از خود، واداشتن دولت مسئول به پیروی از تعهداتش و

جبران خسارت دولت زیان‌دیده است. با توجه به این‌که این حملات سایبری مصداقی از توسل به‌زور و مداخله در امور داخلی دولت محسوب می‌شود، در صورت وقوع یک حمله سایبری که نقض تعهد توسط یک دولت محسوب می‌شود، دولت زیان‌دیده می‌تواند اقدامات متقابل انجام دهد. اقدام متقابل دربرگیرنده اقدامات غیر خصمانه‌ای است که به‌خودی‌خود غیرقانونی است؛ اما زمانی که دولت زیان‌دیده در پاسخ به فعل متخلفانه دولت مسئول به این اقدامات مبادرت می‌ورزد، جنبه غیرقانونی آن زایل می‌شود (خلیل زاده، ۱۳۹۳: ۵۸).

ارائه مدل مفهومی:

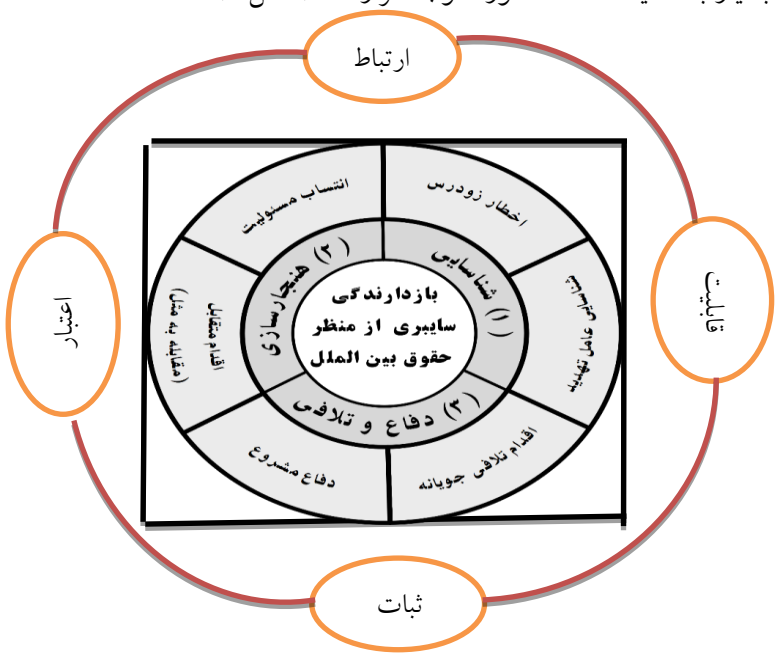
به‌منظور سرعت و دقت در فیش‌برداری و جمع‌بندی مفاهیم، کلیه مستندات جمع‌آوری‌شده، در نرم‌افزار مکس‌کیودا درج گردید و با استخراج مفاهیم مرتبط، کدگذاری و مقوله سازی‌های لازم در چندین مرحله انجام شد (شکل ۱).



شکل ۱ : استخراج عوامل اثرگذار توسط نرم‌افزار مکس کیودا

با استخراج مقوله‌های محوری در نرم‌افزار مکس‌کیو دی‌ای، می‌توان مدل مفهومی الگوی بازدارندگی سایبری را از سه بُعد شامل شناسایی (شناسایی عامل تهدید و اخطار زودرس)، هنجارسازی (انتساب مسئولیت، اقدام متقابل یا مقابله به‌مثل)؛ و دفاع و

تلافی(دفاع مشروع و اقدام تلافی‌جویانه) و مؤلفه‌های چهارگانه (قابلیت، ثبات، اعتبار و ارتباط) و شاخص‌های مربوطه که در بازدارندگی سایبری از منظر ملاحظات حقوق بین‌المللی بسیار با اهمیت هستند، مورد توجه قرار داد (شکل ۲).



شکل ۲: مدل مفهومی پژوهش

۲. روش‌شناسی تحقیق

روش تحقیق در این پژوهش مبتنی بر استدلال استقرایی است چراکه هدف کلی الگوسازی است. استقرا به معنای رسیدن از جزء به کل(الگو) است. در این شیوه استدلال، با استفاده از معلومات جزئی و داده‌های تجربی و برقراری ارتباط بین آن‌ها مدل کلی استخراج می‌شود. پژوهش حاضر مبتنی بر پارادایم تفسیرگرایی و به روش آمیخته (کیفی-کمی) انجام‌شده است. در وهله نخست، از طریق استخراج اطلاعات از منابع گوناگون، به توصیف شرایط و ویژگی‌های بازدارندگی پرداخته‌شده است و سپس با جمع‌آوری منابع

شناخته‌شده و معتبر و درج آن‌ها در نرم‌افزار تحلیل کیفی مکس کیودا[1] ضمن استخراج مفاهیم قابل‌توجه و کدگذاری و مقوله‌سازی از آن‌ها در چندین مرحله، عوامل اثرگذار در «بازدارندگی سایبری از دیدگاه موازین حقوق بین‌الملل» در قالب ابعاد، مؤلفه‌ها و شاخص‌ها احصاء و مدل مفهومی پژوهش ترسیم می‌گردد.

در ادامه نیز به‌منظور خبره سنجی عوامل احصاء شده، مدل معادلات ساختاری مربوطه را در نرم‌افزار تحلیل کمی اسمارت پی.ال.اس[2] ترسیم گردید و پرسشنامه‌ای نیز بر آن اساس تنظیم شد و در بین ۳۰ نفر از خبرگان توزیع شد. درنهایت نیز با جمع‌آوری ۲۸ پرسشنامه و تجزیه‌وتحلیل آن‌ها در نرم‌افزار فوق، با به‌دست آمدن مقدار آن برای برازش کلی، مدل ساختاری مورد قبول واقع شد و ضمن اعمال اصلاحات پیشنهادی خبرگان از طریق استدلالی قیاسی، ابعاد، مؤلفه‌ها و شاخص‌های بازدارندگی سایبری از دیدگاه موازین حقوق بین‌الملل ارائه گردید.

۳. تجزیه و تحلیل یافته‌ها

پژوهش حاضر، باهدف شناسایی الگوی بازدارندگی سایبری شامل ابعاد، مؤلفه‌ها و شاخص‌های از دیدگاه موازین حقوق بین‌الملل به جمع‌آوری و مطالعه مستندات مرتبط پرداخته و با کدگذاری و مقوله سازی از مفاهیم قابل‌توجه توسط نرم‌افزار تحلیل کیفی مکس‌کیودا، عوامل قابل‌توجه را احصاء و مدل مفهومی پژوهش را ترسیم نمود. در ادامه نیز با ترسیم مدل معادلات ساختاری، عوامل فوق در نرم‌افزار اسمارت پی.ال.اس، پرسشنامه‌ای براساس طیف لیکرت ۵ گزینه‌ای (۱=خیلی کم، ۲=کم، ۳=متوسط، ٤=زیاد، ۵=خیلی زیاد) تنظیم و در بین ۳۰ نفر از صاحب‌نظران حوزه پژوهش توزیع و درنهایت نیز ۲۸ پاسخ جمع‌آوری نمود. با تجزیه‌وتحلیل مدل معادلات ساختاری فوق براساس نظر پاسخگویان و به روش مجذور مربعات جزئی، مقدار ۰,۳۹۰ برای برازش کلی به دست آمد که نشان‌دهنده تأیید قوی مدل است لذا، با اعمال اصلاحات مبتنی بر نتایج تجزیه‌وتحلیل کیفی

---

[1] MaxQDA 2020

[2] SmartPLS

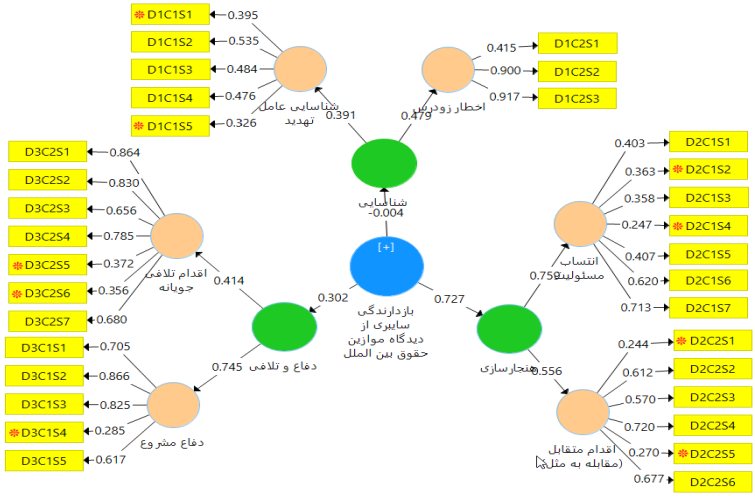
و نظر پاسخگویان، ابعاد، مؤلفه‌ها و شاخص‌های «بازدارندگی سایبری از دیدگاه موازین حقوق بین‌الملل» طبق جدول زیر احصاء و ارائه می‌گردد.

جدول ۱ : ابعاد، مؤلفه‌ها و شاخص‌های احصاء شده از مبانی نظری و مستندات مطالعه شده

بعد		مؤلفه		شاخص	
کد	عنوان	کد	عنوان	کد	عنوان
D1	شناسایی	D1C1	شناسایی عامل تهدید	D1C1S1	شناسایی ابزار، زیرساخت و سلاح‌های استفاده‌شده
				D1C1S2	ادراک خطر از طریق رصد یک یا چند شبکه میانی
				D1C1S3	شناسایی و گرفتارسازی غیرقابل‌انکار تهدیدکننده و یا مهاجم
				D1C1S4	شناسایی انگیزه و قصد کاربران خصوصی و گروه‌های مختلف
				D1C1S5	توجه به ماهیت گمنامی عامل تهدیدکننده و مخفی بودن هویت
		D1C2	اخطار زودرس	D1C2S1	اخطار دهی سریع حمله سایبری کشف‌شده در شرایط بحرانی
				D1C2S2	اخطار دهی سریع حملات و نفوذ در رایانه‌های آسیب‌پذیر
				D1C2S3	اخطار دهی مداوم پیامدهای مشاهده‌شده به‌مرورزمان
D2	هنجارسازی	D2C1	انتساب مسئولیت	D2C1S1	انتساب غیرقابل‌انکار به دلیل گمنامی و مبهم بودن فعالیت سایبری
				D2C1S2	تعیین مالک، مکان فیزیکی و مسئول کار با رایانه مهاجم
				D2C1S3	تعیین موقعیت جغرافیایی و هویت فردی مهاجمان
				D2C1S4	تعیین ویژگی‌های حمله‌ای برای شناسایی گروه خاصی از افراد
				D2C1S5	انتساب به تجاوز یا توسل به‌زور و یا مداخله در امور داخلی
				D2C1S6	انتساب اقدامات به دولت و طرح مسئولیت بین‌المللی
				D2C1S7	انتساب به دولت در صورت حمله توسط افراد در استخدام و کنترل
		D2C2	اقدام متقابل (مقابله‌به‌مثل)	D2C2S1	اقدامات غیر خصمانه در پاسخ به فعل متخلفانه دشمن
				D2C2S2	اقدام طبق مواد ٤٩ تا ٥٣ پیش‌نویس مسئولیت بین‌المللی
				D2C2S3	اقدام متقابل دولت زیان‌دیده در مقابل نقض تعهد توسط یک دولت دیگر
				D2C2S4	واداشتن دولت متخاصم برای پیروی از تعهدات خود و جبران خسارت
				D2C2S5	تنها دولت زیان‌دیده می‌تواند علیه دولت مسئول اقدام متقابل نماید
				D2C2S6	انطباق با اصول و قواعد حقوق بشردوستانه و پرهیز از توسل به‌زور
D3	دفاع و تلافی	D3C1	دفاع مشروع	D3C1S1	رعایت چارچوب حقوق جنگ در دفاع مشروع
				D3C1S2	دفاع مقابل حمله دولت متجاوز نه اشخاص خصوصی یا هر نهاد دیگر
				D3C1S3	پاسخ مشروع متفاوت به تهاجم براساس دولتی یا غیردولتی بودن منشأ
				D3C1S4	برقراری ارتباط میان حمله و منبع طبق حقوق بین‌الملل توسط دولت‌ها
				D3C1S5	فقط قابل‌اعمال برای دولت‌ها نه اشخاص (بند ٤ ماده ۲ منشور–توسل به‌زور)

بعد		مؤلفه		شاخص	
کد	عنوان	کد	عنوان	کد	عنوان
		D3C2	اقدام تلافی‌جویانه	D3C2S1	انجام اقدامات تلافی‌جویانه‌فقط علیه اهداف و پرسنل نظامی و به عنوان آخرین چاره
				D3C2S2	القای ترس از انجام اقدامات تلافی‌جویانه در حوزه بازدارندگی
				D3C2S3	به‌منظور برقراری حاکمیت قانون و نه‌فقط مجازات خاطی
				D3C2S4	متناسب با خطای دشمن و هم‌زمان در فضای واقعی و مجازی
				D3C2S5	تصمیم‌گیری انجام اقدامات تلافی‌جویانه در بالاترین سطح دولتی
				D3C2S6	توقف اقدامات تلافی‌جویانه به‌محض اتمام اقدام خصمانه دشمن
				D3C2S7	چالش‌برانگیز بودن اقدامات تلافی‌جویانه در حقوق مخاصمات مسلحانه

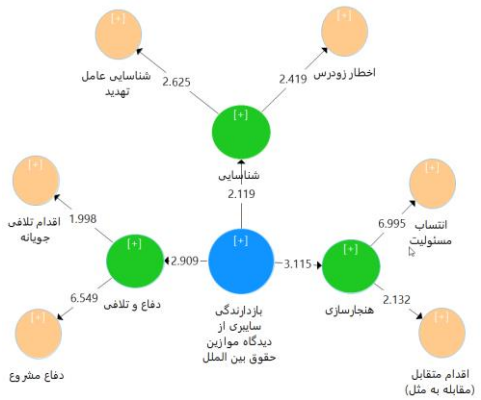
به‌منظور اخذ نظر خبرگان جهت ارزیابی مدل مفهومی احصاء شده از جمع‌بندی ادبیات و مبانی نظری پژوهش، ابتدا مدل معادلات ساختاری مربوطه در نرم‌افزار اسمارت پی.ال.اس و پرسشنامه‌ای براساس طیف لیکرت ۵ گزینه‌ای (۱=خیلی کم، ۲=کم، ۳=متوسط، ٤=زیاد، ۵=خیلی زیاد) بر آن اساس تنظیم گردید.



شکل ۳: مدل معادلات ساختاری

پرسشنامه فوق در اختیار ۳۰ نفر از صاحب‌نظران قرار گرفت (کاغذی و الکترونیکی) و در نهایت نیز ۲۸ پرسشنامه جمع‌آوری شد. ۵۸ درصد از پاسخگویان آشنایی خود را متوسط و ۳۰ درصد زیاد و ۱۲ درصد خیلی زیاد اعلام نموده‌اند و این مطلب دور از انتظار نبود ولی باید توجه داشت که محققین معمولاً خود را پایین‌تر از میزان واقعی در نظر

می‌گیرند. ۳۲ درصد از پاسخگویان، سابقه کار ۱۱ تا ۱۵ سال و ۳۲ درصد دیگر نیز سابقه کار ٦ تا ۱۰ سال را داشته‌اند که بیشترین فراوانی را تشکیل می‌دهند. ٤۳ درصد از پاسخگویان کارشناس فنی، ۲۱ درصد مدیر عملیاتی، ۱۸ درصد عضو هیئت‌علمی، ۱۱ درصد مدیر راهبردی و ۷ درصد نیز مدیر میانی بوده‌اند. مدل ساختاری فوق ، از ۳ جنبه برازش اندازه‌گیری (پایایی)، برازش ساختاری و برازش کلی، طبق روش مجذور مربعات جزئی مورد ارزیابی قرار گیرد. برازش اندازه‌گیری به‌منظور تشخیص صحت شاخص‌هایی تعیین‌شده برای مؤلفه‌ها انجام می‌شود و به‌عبارت‌دیگر، پایایی مدل را از ۳ دیدگاه بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی ارزیابی می‌کند. آلفای کرونباخ و پایایی ترکیبی باید مقادیر بالای ۰,۷ داشته باشند که در محاسبه اولیه مقادیر مناسب نبود ولی از طرف دیگر، بارهای عاملی (اعداد محاسبه و درج‌شده بر روی پیکان‌های متصل به مستطیل در شکل ۳) نباید کمتر از ۰/٤ باشند و مقادیر کمتر از مقدار به این معنا است که پاسخگویان شاخص‌های فوق را مناسب تشخیص نداده‌اند، لذا شاخص‌هایی که با علامت * در شکل ۱ علامت‌گذاری شده‌اند، حذف شد و مقادیر آلفای کرونباخ و پایایی ترکیبی مقادیر بالای ۰,۷ کسب نموده و برازش اندازه‌گیری مدل تأیید شد. به‌منظور ارزیابی برازش ساختاری یا روابط بین متغیرهای پنهان (دایره‌ها)، محاسبات بوت استرپینگ[1] یا خود راه‌اندازی انجام شد (شکل٤).



شکل ٤: محاسبات بوت استرپینگ یا خود راه‌اندازی

[1] BootStrapping

ضرایب معناداری z (اعداد ذکرشده بر روی فلش‌های در شکل ٤) معناداری روابط بین ابعاد و مؤلفه‌های احصاء شده را مشخص می‌کند و مقادیر بیشتر از ۱,۹۶ و بیشتر از ۲,۵۸ و بیشتر از ۳,۲۷، نشان‌دهنده سطح معناداری ۹۵٪ و ۹۹٪ و ۹۹,۹٪ در رابطه بین عوامل است. طبق شکل ٤، همه روابط از معناداری مناسبی برخوردار هستند. در ادامه معیار R Squares یا R^2 یا ضریب تعیین، که میزان تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا را نشان می‌دهد و معیار Q[1] که نشان‌دهنده قدرت پیش‌بینی مدل است مورد ارزیابی قرار گرفتند و میزان متوسط تا قوی را نشان دادند. درنهایت نیز، به‌منظور بررسی برازش یا معیار GOF، جذر حاصل‌ضرب میانگین «متوسط مشترک AVE»[2] و میانگین «ضریب تعیین R2» محاسبه گردید و مقدار ۰,۰۱ و ۰,۲۵ و ۰,۳٦، برازش ضعیف، متوسط و قوی مدل را نشان می‌دهد.

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{۰.۶۲۲ \times ۰.۲۴۵} = ۰.۳۹۰$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰,۳۹۰ بوده و چون از ۰,۳٦ بیشتر است، برازش مدل را قوی ارزیابی نموده و با استفاده از نتایج حاصل قابل‌اتکا می‌باشد.

طبق نتایج پژوهش، از دیدگاه موازین حقوق بین‌الملل، الگوی بازدارندگی سایبری را باید از ۳ بُعد شناسایی، هنجارسازی و دفاع و تلافی موردتوجه قرار داد:

۱) **شناسایی**: قواعد و مقررات حاکم بر مخاصمات مسلحانه ایجاب می‌کنند کشورهایی که به کشوری دیگری حمله می‌کنند نیت خود را اعلام کنند (اخطار دهی)، اگرچه ظاهراً این امر بیش از آن‌که رعایت گردد، نقض شده است. نقض این قاعده و سایر مقررات و رسوم جنگ در هریک از عرصه‌های منازعه، موجد نظام مسئولیت

[1] Stone-Geisser Criterion

[2] Communality: این عنوان به‌صورت مشخص در نسخه ۲ نرم‌افزار وجود دارد ولی در نسخه ۳ نرم‌افزار از مقدارAVE استفاده می شود.

بین‌المللی برای طرف خاطی خواهد شد لذا می‌توان دو مؤلفه را در این خصوص موردتوجه قرار داد:

- **شناسایی عامل تهدید:** با رصد یک یا چند شبکه میانی می‌توان درک صحیحی از خطر کسب نمود و تهدیدکننده و یا مهاجم را به‌صورت غیرقابل‌انکار شناسایی و گرفتار نمود و با شناخت انگیزه و قصد کاربران خصوصی و گروه‌های مختلف، از اهداف آن‌ها آگاه شد.
- **اخطار زودرس:** به‌منظور کاهش اثر حملات، لازم است که سریعاً حمله سایبری کشف‌شده در شرایط بحرانی و پیامدهای مشاهده‌شده به‌مرور زمان به‌طور مداوم اخطاردهی شود تا از نفوذ در رایانه‌های آسیب‌پذیر پیش‌گیری گردد.

۲) **هنجارسازی:** انتساب حمله سایبری به عامل واقعی آن (دولت یا ارکان دولت)، از عناصر اساسی نظام مسئولیت بین‌المللی بشمار می‌رود. «طرح پیش‌نویس مواد کمیسیون حقوق بین‌الملل»[۱] در مورد این قاعده مهم عنوان داشته است که «رفتار هر ارگان از یک دولت طبق حقوق بین‌الملل به عنوان عمل آن دولت محسوب می‌شود، یک ارگان شامل هر شخص یا نهادی است که مطابق با قوانین داخلی کشور دارای چنین وضعیتی است»[۲]. یکی از چالش‌های منحصربه‌فرد در خصوص انتساب حملات سایبری، تعیین این موضوع است که آیا مهاجم یک دولت خارجی، یک سازمان جنایتکار یا تروریستی یا ترکیبی از این‌ها بوده است. بازدارندگی در مقابل یک دولت با بازدارندگی از یک گروه تروریستی متفاوت است و شیوه‌های تلافی‌جویانه و اقدامات متقابل نیز متفاوت است. این امر را می‌توان با اشکال جنگ متعارف مقایسه کرد. اگر یک ارتش خارجی با نیروی نظامی به کشوری حمله کند، دولت موردحمله با هیچ مشکلی در تعیین اینکه چه کسی حمله را انجام داده است، مواجه نخواهد شد و

---

[۱] طرح پیش نویس کمیسیون حقوق بین الملل راجع به مسئولیت بین المللی دولت ۲۰۰۱ که توسط مجمع عمومی سازمان ملل به تصویب رسید.

[۲] Report of the International Law Commission to the General Assembly, 2001

همچنین در مورد میزان مسئولیت آن کشور در حمله هیچ تردیدی وجود نخواهد داشت. در این وضعیت و قبل از اقدام به مقابله‌به‌مثل، کشور قربانی نیازی به اثبات این امر که حمله توسط نیروی نظامی کشور دیگری انجام‌شده است، نخواهد داشت. اما در صورت وقوع یک حمله سایبری، کشور قربانی نه‌تنها باید موقعیت جغرافیایی مهاجمان سایبری را تعیین کنند، بلکه همچنین باید میزان نقش دولتی که حمله سایبری از قلمروی وی وقوع یافته را نیز در حملات تعیین کنند. در این راستا، دو مؤلفه را می‌توان موردتوجه قرار داد:

- **انتساب مسئولیت:** نظر به گمنامی و مبهم بودن فعالیت سایبری،لازم است که انتساب مسئولیت غیرقابل‌انکار حمله انجام‌شده و موقعیت جغرافیایی و هویت فردی مهاجمان مشخص گردد. اگر حمله توسط افراد در استخدام و کنترل یک دولت انجام‌شده باشد، انتساب به دولت و طرح مسئولیت بین‌المللی تجاوز یا توسل به‌زور و یا مداخله در امور داخلی و غیره طرح می‌گردد.
- **اقدام متقابل (مقابله‌به‌مثل):** طرح پیش‌نویس کمیسیون حقوق بین‌الملل، عمل شخص یا گروهی را در حالتی به یک دولت تحت قوانین بین‌المللی نسبت می‌دهد که درواقع شخص یا گروه مزبور در انجام این عمل با دستورالعمل یا تحت نظارت یا کنترل آن دولت عمل می‌کنند. ازاین‌رو اقدامات این گروه قابل انتساب به آن دولت است و طبق مواد ٤٩ تا ٥٣ پیش‌نویس مسئولیت بین‌المللی و منطبق با اصول و قواعد حقوق بشردوستانه و پرهیز از توسل به‌زور، دولت زیان‌دیده در مقابل نقض تعهد توسط یک دولت دیگر اقدام متقابل انجام داده و دولت متخاصم را وادار به پیروی از تعهدات خود و جبران خسارت نماید.
- **دفاع مشروع:** در مرحله نخست، با رعایت چارچوب حقوق جنگ در دفاع مشروع، باید دفاع مقابل حمله دولت متجاوز و نه اشخاص خصوصی یا هر نهاد دیگر را با در نظر گرفتن منشأ دولتی یا غیردولتی بودن حمله انجام داد (طبق بند ٤ ماده ٢ منشور- توسل به‌زور).

- **اقدام تلافی‌جویانه**: اقدامات تلافی‌جویانه در حقوق مخاصمات مسلحانه چالش‌برانگیز ولی اگر از دفاع مشروع نتیجه مورد انتظار حاصل نشد، به عنوان آخرین چاره می‌توان ، اقدامات تلافی‌جویانه را به‌منظور برقراری حاکمیت قانون و نه‌فقط مجازات خاطی، فقط علیه اهداف و پرسنل نظامی دولت متجاوز انجام داد و با القای ترس از در حوزه بازدارندگی و متناسب با خطای دشمن، هم‌زمان در دو فضای واقعی و مجازی انجام داد.

٤. نتیجه‌گیری

امروزه دولت‌ها به‌طور فزاینده‌ای به فضای سایبری وابستگی پیداکرده‌اند، چراکه از طریق آن خدمات عمومی را ارائه و مدیریت می‌نمایند. این در حالی است که از زمان ظهور اینترنت در دهه‌های پایانی قرن میلادی گذشته تمام کاربران فضای سایبری با نیت و اهداف صلح‌جویانه رفتار نکرده‌اند. اکنون فضای سایبری در کنار زمین، دریا، هوا و فضا به عنوان صحنه‌ای جدید برای نبرد پدیدار گشته است. بازدارندگی سایبری محدود به بازداشتن دشمن از به‌کارگیری تهدید سایبری علیه دارایی‌های سایبری نیست، بلکه اعم از آن بوده و به معنای بازداشتن دشمن از هرگونه تهدید سایبری و غیرسایبری علیه هرگونه دارایی سایبری و غیرسایبری با استفاده از کلیه امکانات و با توجه به اقتضائات فضای سایبری و غیرسایبری است. لازم به ذکر است که مقصود از دارایی‌های غیرسایبری، کلیه مولفه‌های قدرت در فضای حقیقی تحت حاکمیت کشورهاست که در حوزه‌های اقتصاد و تجارت، سلامت و ایمنی عمومی، علم و فناوری، فرهنگی و اجتماعی، دفاعی، روابط بین‌المللی تجلی می‌یابد. این نوع دارایی‌ها توسط قابلیت‌های سایبری مورد تهاجم و حمله قرار می‌گیرد بدون اینکه مهاجم ردپایی از خود بجای بگذارد و شناسایی شود.

مسئله پیچیده این واقعیت است که بسیاری از چالش‌های مربوط به انتساب حملات سایبری به مهاجم، اساساً به ماهیت ساختار فضای سایبری برمی‌گردد. عدم توانایی در

انتساب حملات سایبری، دولت‌های قربانی را در تعیین واکنش‌های قانونی تحت مقررات حقوق مخاصمات مسلحانه بین‌المللی با چالش روبرو می‌نماید. اگر دولت قربانی قادر نباشد به نحو متقاعدکننده‌ای اثبات نماید که مهاجم سایبری یک کشور یا سازمان جنایتکارانه یا یک نهاد (شخص) تروریستی بوده است، نمی‌تواند از ظرفیت‌های قانونی یا گزینه‌های مجاز برای واکنش تحت مقررات بین‌المللی استفاده کند. ازاین‌رو، به‌نظر می‌رسد تا فرآیند انتساب بدرستی تبیین نشود، نظریه بازدارندگی سایبری نیز نمی‌تواند کارایی لازم را داشته باشد و توسل به بازدارندگی صرف نمی‌تواند راه‌حل نهایی برای جرائم سایبری، جاسوسی و حملات سایبری باشد و تهدید کننده سایبری را از اهداف خودش منصرف سازد.

پژوهش حاضر نشان داد به دلیل عدم وجود توانایی در شناسایی دقیق عامل واقعی حملات سایبری، در اکثر مواقع، دولت‌های نمی‌توانند به مؤلفه‌های بازدارندگی علیه مهاجمان بالقوه اتکا کنند. حتی اگر دولت قربانی قادر به انتساب حملات سایبری به مهاجم خاصی به نحوی باشد که بتواند مراجع قضایی بین‌المللی را درخصوص عامل واقعی حملات متقاعد نماید، هنوز چالش‌های مربوط به نحوه و چگونگی اعمال مقررات حقوق مخاصمان مسلحانه بین‌المللی در فضای سایبری، و توسل به اقدامات تلافی‌جویانه به قوت خود باقی خواهد بود. بنابراین، تا زمانی که گزینه‌های پاسخگویی در فضای سایبری نامشخص و به‌طور قابل‌توجهی توسط مقررات حقوق مخاصمات مسلحانه محدود شده باشد، تعیین اینکه چه کسی حمله کرده مشکل است و توسل به اقدامات متقابل و اقدامات تلافی‌جویانه به دلیل مسئله انتساب محدود می‌باشد. ازاین‌رو، پیشنهاد می‌شود که برای حصول بازدارندگی مؤثر در فضای سایبر، باید بر قابلیت‌های «شناسایی» و «هنجارسازی» تکیه نمود.

فهرست منابع و مآخذ

الف. منابع فارسی

- اسماعیلی، احسان (۱۳۹۳). ***در جستجوی یک نظام حقوقی برای ستیز سایبری***. پایان نامه کارشناسی ارشد. دانشگاه آزاد اسلامی واحد تهران مرکزی، دانشکده حقوق.
- افتخاری، اصغر (۱۳۸۲). ***استراتژی ملی برای تأمین امنیت در فضای مجازی***، چاپ اول، تهران: انتشارات پژوهشکده مطالعات.
- برادران، نازنین و حبیبی، همایون (۱۳۹٦). ***«قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری»***، مجله مطالعات حقوق عمومی، دوره ٤۹، شماره ۱، ۱۳۹– ۱۵۸.
- جلالی فراهانی، غلامرضا و بیک پوری، محمدصادق (۱۳۹۷). ***«توسعه مفهوم نظریه بازدارندگی در فضای سایبری کشور براساس اسناد بالادستی و رویکردهای موجود»***، نشریه علمی پدافند الکترونیکی و سایبری، سال هشتم، شماره ٤، ۱٦۱–۱۷۳.
- حسینی، پرویز و ظریف‌منش، حسین (۱۳۹۲). ***«مطالعه تطبیقی ساختار دفاع سایبری کشورها»***، فصلنامه پژوهش‌های حفاظتی ـ امنیتی، سال دوم، شماره ۵، ٤۱–٦۸.
- حسینی، محمدرضا (۱۳۹۰). ***«حملات سایبری از منظر قواعد و مقررات حقوق بین‌الملل و حقوق بشردوستانه»***، ***نخستین همایش دفاع سایبری***، پژوهشکده فناوری اطلاعات و ارتباطات، سازمان جهاد دانشگاهی، ۲۵۷ – ۲٦٦.
- خلیل زاده، مونا؛ شعبانی، امید و اقبالی، میثم (۱۳۹۳). ***«جایگاه اقدامات متقابل در برابر حملات سایبری از منظر حقوق بین‌الملل»***، مطالعات بین‌المللی پلیس، بهار ،۱۳۹۳ ، شماره ۱۷، ٤۲–۷۱.
- دهقانی، علی اصغر (۱۳۹٦). «بازدارندگی سایبری در امنیت نوی جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا»، ***مجله رهیافت‌های سیاسی و بین المللی***، سال هشتم تابستان ۱۳۹٦ شماره ٤ (پیاپی ۵۰)، ۱۲۱– ۱٤۷.
- رمضان زاده، مجتبی؛ غیوری ثالث، مجید؛ احمدوند، علی‌محمد و آقایی، محسن(۱۳۹۹). ***«ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر ُبعد بازدارندگی سایبری»***، نشریه مدیریت نظامی؛ تابستان، شماره ۷۸، ٦۱ – ۹۲.
- زابلی زاده، اردشیر و وهاب پور، پیمان (۱۳۹۷). ***«قدرت بازدارندگی در فضای سایبر»***، دوفصلنامهٔ علمی پژوهشی رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هشتم، شمارهٔ اول،

بهار و تابستان، ۷٤ – ٤۷.

- ضیایی بیگدلی، محمدرضا (۱٤۰۲). ***حقوق بین الملل عمومی***، تهران، نشر کتابخانه گنج دانش، چاپ ۲۱.
- عبدلی، قهرمان(۱۳۹۱). ***نظریه بازی‌ها و کاربردهای آن (بازی‌های با اطـلاعات نـاقص، تکاملی و همکارانه)***، تهران: انتشارات سمت، مرکز تحقیق و توسعه علوم انسانی.
- فریدمن، لاورنس(۱۳۸٦)، ***بازدارندگی***، ترجمه عسکر قهرمانپور، تهران: پژوهشکده مطالعات راهبردی.
- لسانی، سید حسام الدین(۱۳۹۵). ***«تعهد دولت‌ها مبنی بر بازبینی حقوقی تسلیحات جدید در حقوق بین‌الملل»***، فصلنامه مطالعات حقوق عمومی، دوره چهل و ششم، شماره ۱، ۹۱ – ۱۱٤.
- لویس، ای. جیمز و حاجی رستملو، قدرت (۱۳۹۲). ***«معارضه در فضای سایبری»***، فصلنامه رصد جنگ نرم، تابستان، شماره ۲، ۱٤۷–۱۵٦.
- ملایی، علی؛ کارگری، مهرداد و خراشادی زاده، محمدرضا (۱۳۹۷). ***«الگوی بازدارندگی در فضای سایبر براساس نظریه بازیها»، فصلنامه امنیت ملی***، سال هشتم، شماره ۲۹، ۱٤۱– ۱۷۲.

ب. منابع انگلیسی

- Bar, S. (2008). "**Deterring Terrorists. Hoover Institution**", available at: http://www.hoover.org/publications/policy-review/article/5674
- Davis, K. & Jenkins, B. M. (2002). "Deterrence &Influence in Counterterrorism: A Component in the War on Al Qaeda". Santa Monica, ***CA: RAND Corp***. 1-99.
- Emilio. Iasiello, (2014). "Is Cyber Deterrence an Illusory Course of Action?", ***Journal of Strategic Security***. Vol. 7 (1).54-67.
- Geer, Jr., D. E. (2007). "**The Physics of Digital Law: Searching for Counterintuitive Analogies**". New York: NYU Press.
- Goldsmith, J., Wu, T. (2006). "**Who Controls the Internet? Illusions of a Borderless World**", oxford: oxford University Press.
- Jasper. Scott, "Deterring Malicious Behavior in Cyberspace", ***Strategic Studies Quarterly***, Vol. 9, No. 1 (SPRING 2015), 60-85.
- Jensen, Eric Talbot. (2012). "Cyber Deterrence", 26 ***Emory Int'l L. Rev.*** 773-791.
- Kesan, Jay & Hayes, Carol. (2011). "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", ***Harvard Journal of Law & Technology.*** Vol. 25 (2). 431-462.

- Knopf, J.W. (2013). "**Use with Caution: The Value and Limits of Deterrence Against Asymmetric Threats**", World Politics Review. https://www.worldpoliticsreview.com
- Libicki, Martin C. (2009). "Cyberdeterrence and Cyberwar", ***RAND Corporation***.
- Lin, Herbert. (2011). "Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion", ***Georgetown Journal of International Affairs***, Special Issue, 127–135.
- Lynn, F. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy", ***Foreign Affairs.*** available at https://www.foreignaffairs.com/print/1113238.
- Morgan, Patrick M. (2010), "**Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,**" paper presented at a workshop on deterring cyberattacks, Washington DC.
- Record, J. (2004). "Nuclear Deterrence, Preventative War, and Counterproliferation", The Cato Institute, ***Policy Analysis***, 1-32.
- Schneider, J. (2016). "**Cyber-Enabled Warfare and Deterrence:** The Capability/Vulnerability Paradox of U.S. Doctrine and Technologies".
- Taipale, K. A. (2010). "Cyber-deterrence", ***Law, Policy and Technology Journal***, IGI Global, World Policy Institute, USA, 298- 315.
- Thomasen, T. (2011). "**Cyber Deterrence** ",21st Century Maginot Line.
- Will, Goodman, (2010). "Cyber Deterrence: Tougher in Theory than in Practice," ***Strategic Studies Quarterly***, Vol.4, No.3 102-135.
- Wirtz, J.J. & Harknett, R. J. (Eds). (2000). "The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order", ***Univ. of Michigan Press***. 189-212.

Documents:

- Agreement on the Prevention of Dangerous Military Activities
- Corfu Channel (U.K v. Alb.), 1949 I.C.J.
- International Telecommunication Convention
- Prosecutor v. Tadic, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, (Oct. 2, 1995)
- Report of the International Law Commission to the General Assembly, 2001
- United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J.