مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
پنجاه و سوم

# مروری بر بازدارندگی سایبری

An Overview of Cyber Deterrence

# گزارش سریع

گزارش شماره۵۳
دی ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

# مروری بر بازدارندگی سایبری

**گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.**


**تهیه شده در پژوهشگاه فضای مجازی**
(گروه حکمرانی فضای مجازی)

نویسنده میهمان: مهدی اکبری
( پژوهشگر هسته سپهرا، مرکز رشد دانشگاه امام صادق علیه‌السلام)
ناظر علمی:
سید امیررضا برقعی دانشجوی دکتری رشته خط مشی‌گذاری عمومی(فضای مجازی)





نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

# فهرست

## فهرست نمودارها

# سخن نخست

# سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

# چکیده

# چکیده

فضـای مجـازی عبـارت اسـت از نظام‌هـای اجتماعـی برآمـده از تعامـل کاربـران بـر بسـتر شـبکه. بنابرایـن بـا شـکل‌گیری نظام‌هـای مختلـف اقتصـادی، فرهنگـی، سیاسـی و ... در ایـن بسـتر، فضای‌مجـازی امتـداد فضـای واقعـی خواهـد بـود و در نتیجـه دولت‌هـا تـلاش خواهنـد کـرد عـلاوه بـر اعمال اقتـدار بر ایـن سـاحت از زندگی شـهروندان خـود، از امنیـت ملـی خـود در ایـن فضا نیـز محافظـت نماینـد. یکـی از مهم‌ترین مفاهیـم موجود در ادبیـات امنیـت، مفهـوم بازدارندگی اسـت. امـروزه و با گسـترش فناوری هـای دیجیتال، شـاهد انـواع تهاجم‌هـا و جنگ‌هـا و جاسوسـی‌های سـایبری نیـز هسـتیم. در مقابـل یکی از راهبـرد هـای مشـهور تامیـن امنیت از دیربـاز، مفهـوم بازدارندگی بـوده اسـت. در گزارش حاضـر، بـا روشـی توصیفـی ـ تحلیلی مبتنی بـر مطالعات کتابخانـه ای به بررسـی مفهوم بازدارندگـی سـایبری، انـواع نظـرات پیرامـون امـکان آن، انـواع راهبـرد هـای ناظـر بـر آن، مسـیرهای پیـش‌روی آن در آینـده و مفاهیـم پیرامونـی آن شـامل قدرت سـایبری، جنگ سـایبری، حملـه سـایبری و دفـاع سـایبری، در ادبیـات علمـی و دانشـگاهی دنیـا پرداخته شـده اسـت. بازدارندگـی بـه معنـای منصـرف کـردن کسـی از انجـام کاری بـا ایجـاد ایـن بـاور در اوسـت کـه هزینه‌هـای ایـن کار از منافـع مـورد انتظـارش فراتـر خواهـد رفـت. سـه مولفـه اساسـی بازدارندگـی سـایبری عبارت اسـت از: سیسـتم دفاعی مسـتحکم برای محافظـت از زیرسـاخت‌ها، توانایـی انتسـاب و شناسـایی مهاجم، تمایل و توانمنـدی تلافی

علیه هر حملهای. در میان دانشمندان، دستهای معتقدند با درک تفاوتهای ماهوی فضای سایبری و واقعی، میتوان راهبردهای زیر را برای بازدارندگی سایبری ارائه کرد: بازدارندگی از طریق انکار، مجازات، وابستگی متقابل و مشروعیتزدایی. البته با توجه به مطالعات انجام شده و تجارب کسب شده در سطح جهان، راهبردی که شامل ترکیبی از موارد چهارگانه فوق باشد، برای ایجاد امنیت و بازدارندگی مناسبتر است. در نهایت، بررسی نقش فناوریهای دیجیتال در روابط میان بازیگران مختلف رقیب در چارچوب بازدارندگی بین حوزهای، تمرکز بر اثرات بازدارندگی سایبری در سطح عملیاتی و تاکتیکی، مورد توجه قرار دادن اجبار به جای بازدارندگی، مفهوم پردازی راهبرد درگیری مداوم و پایدار، چهار مسیر پیش بینی شده برای ادامه مطالعه بازدارندگی در آینده است.

**کلیدواژهها**

**فضایسایبری، امنیت سایبری، بازدارندگی سایبری، دفاع سایبری، تهاجم سایبری، راهبردهای بازدارندگی**

# مقدمه

# مقدمه

فضـای مجـازی عبـارت اسـت از نظام‌هـای اجتماعـی برآمـده از تعامـل کاربـران بـر بسـتر شـبکه (فیروزآبـادی و آزادی، ۱۳۹۹). بـا گذشـت زمـان و توسـعه روز افـزون فناوری‌هـای اطلاعاتـی و ارتباطـی، شـاهد وابسـتگی فـراوان جوامـع بـه ایـن فناوری‌هـا هسـتیم. در نتیجـه هنگامـی کـه کاربـران یـک جامعـه ارتباطـات و تعامـلات خـود را در بسـتر فناوری‌هـای ارتباطـی و اطلاعاتـی شـکل می‌دهنـد، نظام‌هـای اجتماعـی مختلـف اقتصـادی، فرهنگـی، سیاسـی و ... در ایـن فضـا بازتولیـد می‌شـوند. بنابرایـن، همان‌گونـه کـه در فضـای واقعـی، دولت‌هـای ملـی سـعی دارنـد، تـا در قلمـرو حاکمیـت خویـش نسـبت بـه شـهروندان خـود اعمـال اقتـدار نماینـد، در فضـای مجـازی نیـز کـه امـروزه تبدیـل بـه بخشـی از محـل زیسـت شـهروندان گردیـده اسـت، تـلاش دارنـد تـا ایـن اقتـدار را اعمـال نمـوده و حاکمیـت خویـش را هماننـد فضـای واقعـی حفـظ نماینـد. بـه صـورت طبیعـی بخشـی از وظایـف دولـت نسـبت به شـهروندان خـود، فراهـم آوردن شـرایط زیسـت سـالم، امـن و همـراه بـا رفـاه اسـت. گسترش روزافزون فضای مجـازی در کنار آثار مثبتی که در بهبود زیست اجتماعـی بـه همـراه دارد برخی آثـار منفی و قابل توجه دیگری مثـل حملـه سـایبری و جاسوسـی سـایبری را نیز دارد که حتی ممکن است نتایـج آن مخرب تـر

از جنگ های نظامی بوده و امنیت و حیات ملی را به چالش بکشاند. بنابرایـن دولت‌هـای ملـی تـلاش دارنـد، امنیـت ملـی خـود را عـلاوه بـر فضـای واقعـی، در فضـای مجـازی نیـز تامیـن نماینـد. امـا آنچه که در زمینه کنترل فضای مجازی چالش برانگیز است تفاوت ماهوی آن با دنیای واقعی است و همین امر هم کار را بر سیاسـت‌گذاران سخت می‌نمایـد. بـه عبـارت دیگـر، تفاوت‌هایـی کـه اندیشـمندان در مـورد تفاوت‌هـای ماهـوی فضـای واقعـی بـا فضـای مجـازی ذکـر می‌کننـد، باعـث دشـواری بازتولیـد مفاهیـم علمـی، سیاسـت‌گذاری و نهایتـا اجـرا و تامیـن امنیت در ایـن حـوزه شـده اسـت. جهان امروز و آینده ما به یک نظام بین‌المللی جدیدی وارد شده است که آن‌گونـه که باید و شاید، از ظرفیت های تهدید آمیز و همکاری‌جویانه فضای سایبر اطلاع ندارد.[1]

یکـی از مهم‌تریـن مفاهیـم موجـود در زمینـه امنیـت ملـی، مفهـوم بازدارندگی اسـت. از عصـر یونـان باسـتان، بازدارندگـی بخشـی از دکترین امنیتی-سیاسـی کشـورهای غربـی بـوده اسـت. همچنیـن در قـرن معاصـر ایـن راهبـرد، نقـش بسـیار کلیـدی در رویارویـی دو ابرقـدرت آمریـکا و شـوروی در طـول جنـگ سـرد و عصـر سـلاح‌های هسـته‌ای ایفـا کـرده و همچنـان نقـش مهمـی در سیاسـت جهانـی و راهبـرد امنیـت ملـی بسـیاری از کشـورها از جملـه ایـالات متحـده آمریـکا دارد. بـه صـورت متناظـر و بـا توجـه بـه نکاتـی کـه در رابطـه با اهمیـت فضـای مجـازی در عصـر حاضـر ذکـر شـد، مفهـوم راهبـرد بازدارندگی در فضـای سـایبر نیـز می‌بایسـت بازتولیـد شـده و مـورد اسـتفاده قـرار گیـرد. در گـزارش حاضـر، پـس از بررسـی اجمالـی مفاهیمـی چـون قـدرت سـایبری، حملـه و جنـگ سـایبری و دفـاع سـایبری، بـه صـورت تفصیلـی بـه بررسـی ابعـاد مختلـف مفهـوم بازدارندگـی سـایبری پرداختـه خواهـد شـد.

۱. آنچـه امـروز در فضـای نخبگانـی کشـور مـا بـه عنـوان فضـای مجـازی شـناخته میشـود همـان چیـزی اسـت کـه در غرب بـه عنوان فضـای سـایبری معرفـی شـده اسـت (آزادی، ۱۳۹۷). بنابرایـن در ایـن نوشـتار، هـر دو اصطـلاح بـه صـورت متـرداف بـه کار رفتـه اند.

# بخش اول

## قدرت سایبری

# بخش اول

## قدرت سایبری

قدرت سایبری عبارت است از توانایی استفاده از فضای سایبر برای ایجاد مزیت‌ها و تاثیرگذاری بر رویدادها در تمام محیط‌های عملیاتی از طریق ابزارهای قدرت. مفهوم قدرت سایبری را می‌توان در کنار مفاهیمی چون قدرت دریایی، قدرت هوایی، قدرت زمینی و قدرت فضایی بررسی کرد. تعاریف از قدرت، هر چند بسیار مبهم است، اما به نوعی به ظرفیت‌های بالای یک دولت در استفاده از آن به عنوان یک مزیت نسبی اشاره دارد. در حقیقت به هر میزان دولتی بتواند با استفاده از این ظرفیت‌ها به اهداف خود با سریع‌ترین زمان و کم هزینه‌ترین دست پیدا کند، او را می‌توان به عنوان یک قدرت در نظر گرفت. در واقع فضای سایبر میتواند ابزار کسب قدرت اطلاعاتی، اقتصادی، نظامی و سیاسی قرار بگیرد. قدرت سایبر میان دیگر عناصر و ابزارهای قدرت پیوند برقرار می‌سازد و آن‌ها را در جهت نیل به موقعیتی مناسب‌تر یاری می‌رساند. به عبارتی دیگر، فضای سایبر همانند مواد خامی است که سوخت اقتصاد و جامعه را فراهم می کند (اردشیرزاده و وهاب‌پور، ۱۳۹۷). نکته اساسی در این است که برخلاف سایر حوزه‌های قدرت که صرفاً در انحصار بازیگران دولتی قرار داشت، فضای سایبر محدود به بازیگران دولتی نیست. این فناوری اساساً امکان بهره‌گیری برای افراد، سازمان‌های غیردولتی،

جوامع، دانشگاه‌ها و غیره را فراهم آورده است تا از مزیت‌های بسیار منحصرانه‌ای برخوردار شوند(اردشیرزاده و وهاب‌پور، ۱۳۹۷). از این رو، جوزف نای[1] ویژگی قرن جدید را، پراکندگی قدرت می‌داند و اینکه یکی از علل این پراکندگی فضای سایبر است که باعث افزایش تعداد بازیگران شده است(دهقانی، ۱۳۹۶). بنابراین در عصر اطلاعات، دولت‌ها تنها کنشگران بین‌المللی نیستند که ممکن است توانمندی‌های فنی را توسعه دهند تا برای آسیب‌رسانی استفاده کنند، حتی شرکت‌های چندملیتی، سازمان‌های غیردولتی، گروه‌های جنایی و تروریستی و حتی افراد ممکن است دست به عملکردهای جنگی بزنند. از این رو، بررسی تبعات ظهور چنین فضایی بر امنیت ملی کشورها حائز اهمیت است.

۱. جوزف نای (Joseph Nye) دانشمند و پژوهشگر علوم سیاسی آمریکایی و استاد دانشگاه هاروارد است. دستیاری وزارت دفاع و دستیاری معاون وزیر خارجه آمریکا، از مناصبی است که وی تاکنون بر عهده داشته است.
(http://www.irdiplomacy.ir/fa/person/549/جوزف-نای )

# بخش دوم

## حمله و جنگ سایبری

## بخش دوم

# حمله و جنگ سایبری

جنگ سایبری در لغت به معنای تهاجم و حمله بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف جایگزینی، درهم گسیختن، فریفتن، منحط کردن یا تخریب عناصر اطلاعاتی دشمن(اطلاعات، فرآیندهای مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای)(اردشیرزاده و وهاب‌پور، ۱۳۹۷)، در بخش‌های نظامی، شبکه‌های شرکت‌های دولتی یا خصوصی یا هر عنصر زیرساخت حیاتی حاکمیتی(سیستم‌های صنعتی، مالی، تبلیغات، خطوط ارتباطی، شبکه برق و حمل‌ونقل) (بارک‌تُلقا[1]، ۲۰۱۸)، در فضای سایبری است. بنابراین گفتمان رایج در مورد جنگ سایبری بر آسیب‌پذیری «لایه فیزیکی و زیرساختی» فضای سایبری در برابر حملات سایبری تمرکز دارد(سوسانتو و اسمیتس[2]، ۲۰۲۱). البته نتیجه چنین تهاجماتی نه تنها منجر به آسیب فیزیکی به زیرساخت و عملیات فناوری اطلاعات قربانی می‌شود، بلکه می‌تواند عامل تأثیر روانی منفی بر جامعه نیز باشد. چنین عملیاتی به طور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی و غیره انجام می‌پذیرد. بنابراین باید دارای ارزش افزوده و به اصطلاح بهره برداری از عناصر دشمن باشد(اردشیرزاده و وهاب‌پور، ۱۳۹۷).

1.Burak Tolga
2. Soesanto & Smeets

باراک اوباما رئیس جمهور آمریکا در سال ۲۰۱۳ در خصوص ویژگی منحصر به فرد خطراتی که توسط حملات سایبری به زندگی بشر تحمیل می شود، هشدار داد. وی با اشاره به خطراتی که این فضا در اختیار مهاجمان قرار می دهد نوشت: «در منازعه آینده، دشمن قادر به چالش کشیدن برتری نظامی ما نخواهد بود، بلکه به دنبال بهره‌برداری از آسیب پذیری‌های سیستم‌های رایانه‌ای ما در سرزمین‌مان خواهد بود. از کار انداختن سیستم‌های بانکداری حیاتی می‌تواند به یک بحران مالی وحشتناک منجر شود. فقدان آب تمیز و گوارا و یا از کارانداختن کارکرد بیمارستان‌ها میتواند سلامت عمومی ما را به خطر اندازد. و همچنانکه در گذشته شاهد بوده‌ایم، فقدان برق می‌تواند تجارت، شهرها و مناطق منحصر به فرد ما را دچار وقفه کند» (اردشیرزاده و وهاب‌پور، ۱۳۹۷). تهدیدات سایبری در سال ۲۰۰۷ در لیست تهدیدات بزرگ امنیت ملی جایی نداشت. این در حالی است که در سال ۲۰۱۵ اولین رتبه را در لیست مزبور به خود اختصاص داده است(سوسانتو و اسمیتس، ۲۰۲۱). نتیجه اهمیت یافتن روز افزون این مسئله، باعث شده است در سال‌های اخیر حوزه مطالعات سایبر ذیل رشته امنیت بین الملل در فضای دانشگاهی در دنیا شکل گیرد(دهقانی، ۱۳۹۶).

# بخش سوم

## دفاع سایبری

## بخش سوم

## دفاع سایبری

### تفاوت‌های دفاع و حمله در فضای سایبری و واقعی

با توجه به نکاتی که در مورد حمله و جنگ سایبری ذکر گردید، طبیعتاً مفهوم دفاع سایبری نیز اهمیت می‌یابد. اما قبل از پرداختن به مفهوم دفاع سایبری لازم است به برخی ویژگی‌های ماهوی فضای‌سایبر اشاره شود. فضای سایبر بستر مناسبی برای شکل‌گیری آشوب سیاسی و بی‌ثباتی راهبردی است. این فضا ویژگی‌هایی دارد که آن را از عرصه های سنتی متمایز کرده و امکانات مناسبی جهت ایجاد هرج ومرج در اختیار قرار می‌دهد. عمده تفاوت های اساسی حمله و دفاع در فضای سایبری و واقعی به شرح زیر قابل طبقه بندی است(دهقانی، ۱۳۹۶):

۱) غلبه حمله بر دفاع: بر اساس نظریه واقع‌گرایی تهاجمی[۱]، دولت‌ها میل دارند تا در جهت تضمین امنیت خود، در تهاجم از یکدیگر سبقت بگیرند. عرصه سایبر نیز فضایی است که در آن حمله بر دفاع غلبه دارد. در واقع شرایط به گونه ای است که امکانات موجود برای حمله به مراتب بیشتر از دفاع است. در عرصه‌های سنتی، شروع یک حمله (زمینی، هوایی یا دریایی) نیاز به زمینه‌چینی برای تصمیم‌گیری سیاسی داشته و عواقب بین المللی زیادی بر حمله مترتب است، درحالی که در فضای

۱. براساس نظریه واقع‌گرایی در روابط بین‌الملل، ساختار آنارشیک نظام بین‌الملل، کشورها را وامی‌دارد تا در جهت بقای خود اقدام به افزایش قدرت نمایند. قدرت که با توزیع نسبی توانمندی‌های نظامی و اقتصادی در سطح نظام اندازه‌گیری می‌شود، تنها تضمین‌کننده امنیت کشورها محسوب می‌شود. واقع‌گرایی تهاجمی اشعار می‌دارد که قدرت‌های بزرگ در جهت تضمین امنیت خود، همواره به دنبال بیشینه‌سازی درصد سهم خود از قدرت جهانی اند. قدرت فائق بودن، بهترین راه تضمین بقاست، بنابراین دولت‌ها در جهت تهاجم از یکدیگر سبقت می‌گیرند.

سایبر، شروع حمله بدون نیاز به اقدامات اولیه آن چنانی و با هزینه ملی و بین‌المللی پایین صورت می‌گیرد. از طرفی، افزایش حجم و پیچیدگی‌های روزافزون نرم‌افزارها، در واقع حفره‌های امنیتی آن‌ها را افزایش داده و به مهاجمان اجازه می‌دهد که از طریق این حفره‌ها[1] نفوذ کنند. این در حالی است که سیستم‌های قربانی هیچ گونه اطلاعی از این موضوع ندارند. بنابراین، در وضعیت بی اطلاعی مدافعین، امکان دفاع از بین می‌رود. در واقع ماهیت مسئله به گونه ای است که امکان دفاع برای قربانی بسیار محدود است. موضوع غلبه حمله بر دفاع، معمای امنیت[2] را به سه روش تشدید می‌کند:

الف .در اولین وجه، فهم غلبه حمله بر دفاع، مسابقه تسلیحات سایبری بین دولت‌هایی را که بر اساس نظریه واقع‌گرایی تهاجمی به دنبال کسب برتری در این فضای راهبردی هستند، افزایش می‌دهد. هیچ گونه کنترلی بر تولید و انتقال سلاح‌های سایبری وجود ندارد.

ب. دومین وجه تشدید معمای امنیت این است که دارندگان این سلاح‌ها قطعاً از آن‌ها بهره برداری خواهند نمود. برخلاف سلاح‌های هسته‌ای، در شرایط کنونی این‌ها سلاح‌هایی برای استفاده کردن هستند.

ج. سومین وجه مسئله این است که در عرصه سایبر، نظم دفاع-حمله بر هم می‌خورد. در عرصه سنتی، عبور هر کشور از مرزهای طرف مقابل، حمله تلقی می‌شد، ولی در فضای سایبر این گونه نیست و حساسیت‌ها پایین‌تر است. همچنین، موضوعی به نام دفاع فعال وجود دارد که طی آن شما می‌توانید در جهت دفاع و جلوگیری از حمله سایبری، اقدام به ورود به

۱. در اصطلاح فنی به این حفره‌ها Day-Zero Vulnerability گفته می‌شود

2. Security Dilemma

سیستم طرف مقابل کرده و آن را مختل نمایید. لذا در این جا هرکسی که وارد شبکه طرف مقابل می‌شود، می‌تواند مدعی اقدام پیش گیرانه شود.

۲) مسئله انتساب[1] : یافتن منبع حمله غالبا امری دشوار است. سختی تشخیص تعداد مهاجمان، مکان آنها، سختی هماهنگی موثر بین المللی برای یافتن مهاجمان، زمان بر بودن یافتن این مهاجمان از جمله موارد این دشواری است(دهقانی، ۱۳۹۶). اگر قرار است بازدارندگی قبل از انجام اولین اقدام تلافی جویانه عمل کند، دیگران باید اطمینان داشته باشند که دولت بازدارنده متوجه خواهد شد که چه کسی به آن حمله کرده است. تشخیص نادرست مهاجم و ضربه زدن به فرد نامناسب نه تنها منطق بازدارندگی را تضعیف می‌کند بلکه احتمالاً دشمن جدیدی ایجاد می‌کند. مدافع نه تنها باید خود را متقاعد کند، بلکه باید اشخاص ثالث را نیز متقاعد کند که انتساب درست است (بارک‌تُلقا، ۲۰۱۸).

۳) سرعت پیشرفت فناوری: سلاح‌های سایبری و نرم افزارها با آن چنان سرعتی رشد می‌کنند که صرف زمان جهت شناسایی آن‌ها بیهوده است، زیرا به سرعت از دور خارج شده و سلاح‌های جدیدی جای آن‌ها را می‌گیرد. در برخی مواقع، عمر حفره‌های امنیتی در حد چند روز است و به محض کشف، توسط شرکت‌های تولیدکننده نرم افزار شناسایی و پوشش داده می‌شوند. این در حالی است که در فضای سنتی، عمر تسلیحات به ده‌ها سال نیز می‌رسد.

۴) عمق راهبردی کم[2]: چهارمین ویژگی بی‌ثبات‌کننده در فضای

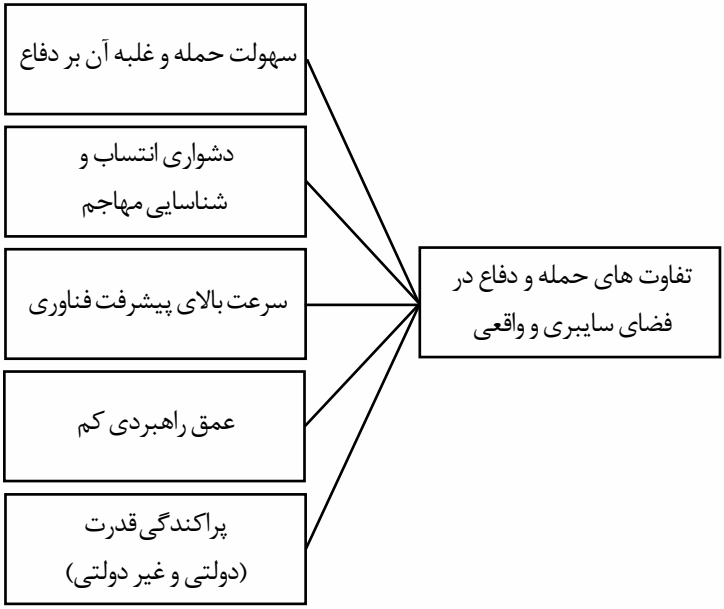
1. Attribution

۲. عمق راهبردی یک واژه در ادبیات نظامی است که به طور گسترده به فاصله بین خط مقدم با بخش‌های نبرد رزمندگان و مناطق اصلی صنعتی، پایتخت‌ها، قلب کشور، و دیگر مراکز اصلی جمعیت و تولید نظامی اطلاق می‌شود
(https://fa.wikipedia.org/wiki/%D%8B%9D%85%9D82%9_%D%8A%7D%8B%3D%8AA%D%8B%1D%8A%7D%8AA%DA%98%DB8%C%DA%A9)

سایبر، زمان کمی است که یک مدافع از لحظه کشف احتمالی حمله تا زمان اتمام آن زمان دارد. دایره زمانی عملکرد تسلیحات سایبری بسیار کوتاه و در حد میلی ثانیه است. در این مهلت محدود، زمانی برای تصمیم‌گیری انسانی و بروکراتیک سازمانی و دفاع وجود ندارد.

۵) پراکندگی قدرت: ویژگی پنجم عبارت است از افزایش تعداد بازیگران و نقش آفرینان اعم از بازیگران دولتی به بازیگران و افراد غیر دولتی؛ در نتیجه، شاهد افزایش پیچیدگی و سختی همکاری و هماهنگی در هر حمله و دفاع، افزایش پیچیدگی و سختی انسجام بین واحدهای مختلف یک دولت برای عمل یکپارچه و منسجم و نهایتاً افزایش قدرت بازیگران غیر دولتی در خارج از دولت در حمله سایبری (مثل افراد یا گروه‌های تبهکار) خواهیم بود. با تمام این اوصاف، این نتیجه حاصل می شود که فضای سایبر ترکیب جدیدی از الگوی زندگی در یک فضای ناشناخته را به بشر ارائه می دهد. این فضا برای تمام بشریت امکان بازیگری را فراهم می‌کند. از کودکان خردسال گرفته تا سازمان‌ها و شرکت‌های چند ملیتی و نیز دولت‌های قدرتمند. فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد. جغرافیا را از بین می‌برد؛ فاعل بودن انسان در محیط اجتماعی را به محیط مجازی بسط می‌دهد؛ ایده‌ها را گسترش می دهد؛ کنترل پذیری را بی‌معنا می‌سازد؛ و دولت را به عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و ... خلع سلاح می‌کند (اردشیرزاده و وهاب‌پور، ۱۳۹۷). در نمودار ۱، به صورت خلاصه، تفاوت‌های حمله و دفاع در فضای واقعی و سایبری ذکر شده است.

نمودار ۱؛ تفاوت های حمله و دفاع در فضای سایبری و فضای واقعی




## عوامل دشواری دفاع سایبری

با توجه به تفاوت های اساسی حمله و دفاع در فضای سایبری و واقعی این مطلب آَشکار می شود که در عرصه سایبر ، دفاع امری بسیار مشکل است و لازم است برای این مسئله تدبیری جایگزین اتخاذ شود. چهار عامل در مسیر دفاع سایبری وجود دارد که عملا اتخاذ راهبرد دفاع در تامین امنیت سایبری را با مشکلات اساسی مواجه می‌سازد(دهقانی، ۱۳۹۶):

۱) اولین عامل، غیرقابل پیش‌بینی و غیرقابل حمله است. چون حمله از طریق حفره‌های امنیتی انجام می‌شود که هنوز توسط شرکت‌های

امنیت سایبری و ویروس یاب‌ها کشف نشده‌اند، قربانی از وجود آن خبری ندارد تا بتواند پیش‌بینی یا کشف حمله کند. به عنوان مثال، گفته می‌شود عامل‌های استاکس‌نت به مدت سه سال در سیستم‌های ایران مقیم بوده و کارشناسان ایران از وجود آن‌ها اطلاعی نداشته‌اند.

۲) دومین مشکل، وجود سطوح پیچیده دفاع است. همانگونه که اشاره شد، پیچیده شدن روزافزون سیستم‌ها، به معنای ازدیاد راه‌های نفوذ نیز هست. با افزایش حجم نرم افزارها در دنیای برنامه‌های کاربردی، در کنار قابلیت‌های بیشتر و ظاهری زیباتر، دفاع نیز سخت‌تر و پیچیده‌تر می‌شود.

۳) سومین عامل، چندتکه شدن دفاع است. در حال حاضر بخشی از شبکه‌های حساس کشورها توسط بخش خصوصی اداره می‌شوند و این بدین معنی است که در هنگام دفاع می‌بایست بین بخش‌های مختلف دولتی و خصوصی هماهنگی به وجود بیاید و این بر مشکلات خواهد افزود.

۴) مشکل چهارم نیز نهایتا، ریسک‌های زنجیره تأمین است. در دنیای کنونی هیچ کشوری زنجیره تأمین اقلام سایبری خود را به صورت کامل در دست نداشته و ضروری است تا بخشی از این تجهیزات از خارج کشور تأمین شوند. در هر مرحله ای از این زنجیره تأمین، سازمان‌های اطلاعاتی خارجی می‌توانند بخشی از سیستم‌ها را بدون اطلاع کشور هدف آلوده کرده و درنتیجه بدافزارهای موردنظر را وارد شبکه آن کنند. پنج عامل برشمرده شده، دفاع را در فضای سایبر به شدت پیچیده و در اکثر مواقع غیرممکن می‌نمایند. با توجه به نکات فوق، کشورهای مختلف راهبرد بازدارندگی را جایگزین

راهبـرد دفاع در اولویت تامین امنیت سـایبری خود قرار داده‌انـد. از این رو، مفهوم بازدارندگی سـایبری در ادامه به صورت تفصیلی مورد بررسـی قرار خواهد گرفت

# بخش چهارم

## بازدارندگی سایبری

## بخش چهارم

### بازدارندگی سایبری

از عصر یونان باستان، بازدارندگی بخشی از دکترین امنیتی-سیاسی کشورهای غربی بوده است. این راهبرد نقش بسیار کلیدی در رویارویی دو ابرقدرت در طول جنگ سرد و عصر سلاح‌های هسته‌ای ایفا کرد و همچنان نقش مهمی در سیاست جهانی داشته و حتی می‌تواند در جهان سایبر نیز به کار گرفته شود. همچنان که در حال حاضر نیز بازدارنگی، عنصر اساسی در راهبرد امنیت ملی دولت آمریکا به شمار می‌رود(اردشیرزاده و وهاب‌پور، ۱۳۹۷). نظریه بازدارندگی کلاسیک محصولی جانبی در دوران جنگ سرد است و توسعه آن بیشتر تحت تاثیر روابط خصمانه ایالات متحده آمریکا و اتحاد جماهیر شوروی و سلاح‌های اتمی بوده است. اما بازدارندگی یک پدیده جهانی است که در ابعاد فرهنگی و فناوری نیز در همه سال‌ها به کار گرفته می‌شود. هدف بازدارندگی در عرصه سایبر کاهش مخاطره حمله سایبری به سطح قابل پذیرش، با هزینه‌ای قابل پذیرش است(ملائی و همکاران، ). البته ریچارد کلارک[1] از اولین اندیشمندان حوزه امنیت سایبری، اعتقاد دارد که از بین تمام مفاهیم راهبرد هسته‌ای، مفهوم بازدارندگی کمترین امکان را برای انتقال به نبرد سایبر دارد و امکان بازتولید و عملیاتی‌سازی این مفهوم در این فضا پایین است. فرمول‌بندی

1. Clarke

یک راهبرد مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی داشته و اشتباه است که در این مسئله حوزه سایبر را تنها در نظر بگیریم. نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری ارائه دهیم. بازدارندگی سایبری به این معناست که در پاسخ به یک حمله سایبری می‌توانیم از طریق تمامی عرصه‌ها پاسخ دهیم. در راهبرد سایبری آمریکا در ۲۰۱۱ تصریح شده است که آمریکا در حوزه سایبری حق استفاده از کلیه ابزارهای دیپلماتیک، اطلاعاتی، نظامی و اقتصادی را برای خود محفوظ می‌داند(دهقانی، ۱۳۹۶).

## تعریف بازدارندگی

« بازدارندگی عبارت است از راهبردی با هدف منصرف کردن دشمن از انجام اقدامی که هنوز شروع نشده یا منصرف کردن دولتی از انجام کاری که دولت دیگری می‌خواهد (او از این اقدامش) منصرف شود؛ یا منصرف کردن کسی از انجام کاری با ایجاد این باور در او که هزینه‌های این کار از منافع مورد انتظارش فراتر خواهد رفت» (نای[1] ، ۲۰۱۷). بازدارندگی نوعی رابطه است که طی آن یک طرف سعی می‌کند با استفاده از وسایلی در رفتار طرف مقابل تاثیر گذارده و به منظور تعقیب هدف یا اهداف خاصی در آن نفوذ نماید. این نفوذ ممکن است از راه‌های گوناگون و در جهت‌های مختلف تامین شود. در بازدارندگی نظامی که نوعی خاصی از اعمال نفوذ مد نظر است، یک طرف، طرف دیگر را تهدید می‌کند که چنانچه در جهت مطلوب عمل نکند، به شدت مجازات خواهد شد. این جهت مطلوب ممکن است حفظ وضع موجود، رفتن به سمت وضعیتی معین و عدم استفاده از قوای نظامی و غیره باشد. بازدارندگی می‌تواند یک جانبه، دو جانبه و یا چند جانبه بوده

1. Nye

و معمولا جلوه فیزیکی و مادی ندارد، بلکه به نحوی احساسی و روانی عمل می‌کند. بازدارندگی غالباً به شکل تفهیم و تفاهم و ارتباط و تبادل اطلاعات و نظریات به طور ضمنی و صریح است. هدف نهایی بازدانگی این است که کشورهای مختلف بتوانند برای حل مسائل و اعمال سیاست‌های خود از روش‌های غیر تهاجمی بهره گرفته و از عملیاتی که منجر به درگیری با کشور دیگری شود، جلوگیری نماید. البته در سیاست بین الملل این اصل پذیرفته شده است که کشمکش جزء اصول اساسی صحنه روابط بین الملل است و باقی نیز خواهد ماند. اما این پذیرش به معنی آن است که باید درگیری‌ها را در حد جنگ‌های محدود و کنترل شده نگه داشت و مانع گسترش آنها شد(مرکز پژوهش‌های مجلس، ۱۳۷۵). بازدارندگی به عنوان یک راهبرد، در پی آن است که متخاصمان را به نحوی تشویق و ترغیب کند تا در پیگیری منافع خویش از انجام برخی اقدامات پرهیز کنند، و در چارچوب سلاح‌های راهبردی نشان می‌دهد که هزینه‌ها و مخاطراتی که ملازم با یک تجاوز نظامی است، فراتر از دستاوردهایی است که معمولا انتظار می‌رود از آن حاصل شود. بازدارندگی هم چنین واجد جنبه‌های روانی است. ژنرال بوفر، تحلیل‌گر و راهبردنگار معروف فرانسوی، می‌گوید: «استراتژی بازدارندگی یک فرآیند روانی است که در آن زور جای مهمی دارد، ولی دارای اهمیت انحصاری نیست. به عبارت دیگر، بازدارندگی دشمن را از نظر فیزیکی دفع نمی‌کند، بلکه به لحاظ روانی از تجاوز او جلوگیری می‌کند». هنری کسینجر در زمینه مفهوم بازدارندگی و بعد روانی آن می‌گوید: «همان طور که قدرت به طرز وحشتناکی رشد کرده، به صورت انتزاعی نامحسوس و اغفال کننده نیز درآمده است. بازدارندگی یک سیاست مسلط نظامی است، اما بیش از هر چیز وابسته به ملاک‌های روانی است. در این

راهبرد سعی می‌شود تا با نشان دادن خطرات غیرقابل تحمل، طرف مخالف را از ارتکاب به عمل بازداشت. پیروزی این سیاست، بستگی به آگاهی کامل از محاسبات طرف مخالف دارد. بلوفی که جدی گرفته می‌شود، به مراتب مؤثرتر از تهدیدی است که به عنوان یک بلوف تلقی می‌شود. برای مقاصد سیاسی، میزان قدرت مؤثر نظامی یک کشور، همان ارزیابی یک کشور دیگر از آن قدرت است. از این رو ملاک‌های روانی کم اهمیت‌تر از نیروهای واقعی نیستند»(دهقانی، ۱۳۹۶). بازدارندگی از نگاه وزارت دفاع آمریکا نیز نفوذ قاطعانه بر محاسبات تصمیم گیری متخاصم به منظور جلوگیری از عمل خصومت‌آمیز علیه منافع حیاتی ایالات متحده تعریف شده است. کشور بازدارنده تصمیم می‌گیرد تا اقدامی انجام نشود زیرا آنها فهمیده‌اند یا درک کرده‌اند که انجام چنین عملی پیامدهای غیرقابل تحملی را به همراه خواهد داشت. البته لازم به ذکر است که ایده تأثیر بر تصمیمات کشورها فرض می‌کند که کشورها بازیگران عاقلی هستند، مایل‌اند تا هزینه‌های درک شده از یک عمل علیه منافع درک شده را اندازه گیری کنند و یک برنامه عمل انتخاب کنند، به صورتی که این برنامه منطقاً مبتنی بر نرخ هزینه و فایده قابل استدلال است(ملائی و همکاران، ۱۳۹۸). بازدارندگی سایبری نیز همانند دیگر بازدارندگی‌ها وقتی موفق خواهد شد که دشمن تصمیم به اقدام خصمانه نمی‌گیرد. این تصمیم از دو ارزیابی جداگانه پیروی می‌کند؛ هزینه‌های تخاصم بیشتر از مزایای آن باشد و مزایای خودداری در فضای سایبر بیشتر از هزینه‌ها باشد. در ادامه مفهوم بازدارندگی در فضای‌سایبر با تفصیل بیشتری مورد بررسی قرار خواهد گرفت.

**مولفه‌های یک راهبرد بازدارندگی**

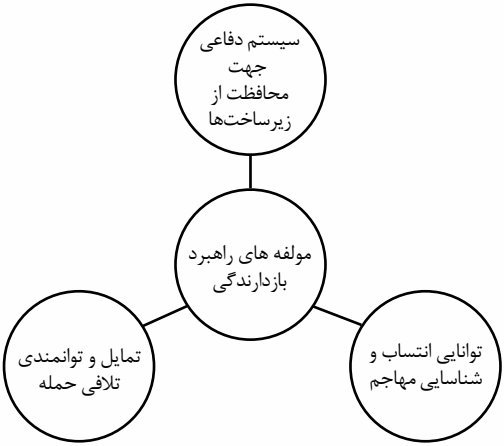
سه مولفه مهم یک راهبرد مناسب بازدارندگی عبارت‌اند از (اردشیرزاده و وهاب‌پور، ۱۳۹۷) (نمودار۲):

۱) دفاع: 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.

۲) انتساب: توان‌مندی مرتبط ساختن حمله‌ای به یک بازیگر یا منبع خاص، عنصر کلیدی دیگری در عرصه سایبری است که اعتبار و مشروعیت بازیگر را در عرصه داخلی و خارجی حفظ می‌کند. علی‌رغم وجود این چالش‌ها در حوزه انتساب، باید به این امر اشاره داشت که این مولفه همچنان بخش کلیدی و اساسی نظریه بازدارندگی در حوزه سایبری هست. تلافی کردن: تمایل و توانمندی تلافی علیه هر حمله‌ای از هر منبعی و تحت هر شرایطی باید ایجاد شود. برای مقابله با بازیگران غیردولتی، اتخاذ اقدامات تلافی‌جویانه متناسب جرم، چالش‌هایی را برای دولت‌ها به‌وجود می‌آورد، چرا که هنوز قوانینی در حقوق بین الملل برای این موضوع تصویب نشده است. به همین منظور، کشورها باید به شدت در این زمینه فعال بوده و دقیقاً اقدامات غیرقانونی را تعریف کنند. این امر می‌تواند در فرآیند قضایی و دادخواهی موثر واقع شود. علی‌رغم چالش حقوقی، مقابله با تهدید بازیگران غیردولتی بسیار حائز اهمیت هست. بسیاری از حملات سایبری روزانه، به دلیل عدم ترس مهاجمان از تلافی است. دولت‌ها اگر در پی کاستن از میزان این حملات مخرب هستند، باید در عمل نشان دهند که مهاجمان از تیغ تلافی

آنها در امان نخواهند بود. برای بیشینه سازی کارآمدی بازدارندگی در حوزه سایبری، دولت‌ها باید آمادگی خود را برای اتخاذ انواع اقدامات تلافی جویانه در حوزه‌های مختلف از تحریم‌های اقتصادی و ضبط اموال کشور مهاجم گرفته تا انواع اقدامات دیپلماتیک و سیاسی و حتی اقدام نظامی نشان دهند. نکته دیگر این است برای امکان اثرگذاری راهبرد بازدارندگی عزم راسخ برای برخورد سریع با مهاجم پس از حمله ضروری است. نیاز به متقاعد کردن دشمن احتمالی وجود دارد که یک حمله سایبری پس از نسبت دادن دقیق به آن، به سرعت رسیدگی خواهد شد. بازیگر بازدارنده باید اراده و عزم خود را برای اقدام در پاسخ به یک حمله سایبری منتقل کند. ایجاد و گسترش اطمینان از قبل در مورد مجازات سریع در صورت وقوع یک حمله سایبری یک راهبرد بازدارنده است. با این حال، عدم اجرای به موقع مجازات به هر دلیلی (یعنی مشکلات انتساب) به اعتبار بازیگر بازدارنده آسیب جدی وارد می‌کند و با هر حمله سایبری بعدی، به صفر نزدیک می‌شود (بارک‌تُلقا، ۲۰۱۸).

نمودار ۲؛ مولفه‌های یک راهبرد بازدارندگی



**معانی بازدارندگی سایبری برحسب نوع ابزار**

امروزه به عنوان یک مفهوم نظامی، بازدارندگی سایبری حداقل سه معنای متفاوت دارد؛ اول، بازدارندگی سایبری می‌تواند به استفاده از ابزار سایبری برای جلوگیری از یک حمله (نظامی) اشاره داشته باشد. دوم، بازدارندگی سایبری می‌تواند به استفاده از ابزار (نظامی) برای جلوگیری از یک حمله سایبری اشاره داشته باشد. سوم، بازدارندگی سایبری می‌تواند به استفاده از ابزار سایبری برای جلوگیری از یک حمله سایبری اشاره داشته باشد. اگرچه به صراحت بیان نشده است، اکثر ادبیات موجود بر دو مفهوم اخیر متمرکز شده‌اند(سوسانتو و اسمیتس، ۲۰۲۱).

**انواع دیدگاه های اندیشمندان در مورد امکان بازدارندگی سایبری**

به صورت کلی می‌توان دیدگاه های اندیشمندان امنیت سایبری در رابطه امکان و نحوه بازدارندگی سایبری را در سه طبقه زیر قرار داد(سوسانتو و اسمیتس، ۲۰۲۱):

۱) گروه اول استدلال می‌کنند که بازدارندگی سایبری مسائل مشخص و متمایزی ندارد و بنابراین همانند بازدارندگی در روابط دنیای واقعی است. این گروه بر این معتقدند که فضای سایبری در ویژگی‌های بسیاری با حوزه‌های سنتی مشترک است و بنابراین بازدارندگی را می‌توان از طریق رژیم‌های موجود به دست آورد. هنجارها و موافقت نامه‌های بین المللی، عامل ایجاد امنیت سایبری بهتر است و بازدارندگی نیز با همان منطق مجازات سنتی می‌تواند اعمال شود.

۲) گروه دوم معتقدند که بازدارندگی سایبری مجموعه منحصر به فرد از مسائل را در بر می‌گیرد، زیرا ماهیت فضای سایبری با حوزه‌های سنتی متفاوت است. بنابراین حل معمای بازدارندگی تنها در صورتی امکان پذیر است که درک بهتری از پویایی‌های اساسی در بازی به دست آوریم. طرفداران بازدارندگی سایبری (چه در گروه اول، چه در گروه دوم) تمایل دارند یکی از چهار منطق بازدارندگی را مورد بحث قرار دهند: ۱- بازدارندگی با انکار،۲- بازدارندگی با مجازات،۳- بازدارندگی با درهم تنیدگی و۴- بازدارندگی توسط مشروعیت زدایی(در ادامه این چهار راهبرد بازدارندگی با تفصیل بیشتری معرفی خواهند شد).

۳) گروه سوم استدلال می‌کنند که یا بازدارندگی سایبری اساسا امکان پذیر نبوده و یا حداقل به روشی که دو گروه اول به آن اعتقاد دارند، امکان پذیر نیست. به اعتقاد برخی از این اندیشمندان فضای‌سایبر با مسائلی از قبیل دشواری رعایت محرمانگی، ضعف عقلانیت و دشواری انتساب روبروست. این اندیشمندان ایده فریب همه جانبه هم در دفاع و هم در حمله را به عنوان راهبرد جایگزین پیشنهاد می‌دهند. برخی دیگر نیز ایده پایداری سایبری را مطرح می‌کنند که در ادامه گزارش به آن پرداخته خواهد شد.

## راهبردهای چهارگانه بازدارنگی سایبری

در این بخش چهار راهبرد اساسی مطرح در ادبیات بازدارندگی سایبری در دنیا که اندیشمندان گروه های اول و دوم به آن ها معتقد هستند، معرفی می‌شوند(سوسانتو و اسمیتس، ۲۰۲۱؛ دهقانی، ۱۳۹۶):

۱) ازدارندگی با **انکار**[1] اساساً مترادف با امنیت سایبری است. در اصل، ایده مفهومی آن این است که ایجاد امنیت سایبری بهتر، احتمال نفوذ شبکه را کاهش می‌دهد و بنابراین بر محاسبات هزینه-فایده یک دشمن تا حدی تأثیر می‌گذارد که یا از حمله جلوگیری می‌کند یا مهاجم را متوقف می‌کند. به عبارت دیگر این راهبرد به این معنی است که اقداماتی انجام شود تا مهاجم به این درک برسد که در صورت اقدام به حمله، نمی تواند تأثیر آن چنانی بر جای گذاشته و نتیجه ای برای او در بر ندارد؛ یا تهاجم او خنثی خواهد شد و یا این تهاجم هزینه زیادی برای وی خواهد داشت. این راهبرد در دوران جنگ سرد و بازدارندگی هسته ای چندان کارا نبود، فلذا ابرقدرت‌ها سلاح‌های خود را در جغرافیای وسیعی پخش کرده بودند که در صورت حمله سریعا پاسخ دهند.

۲) بازدارندگی از طریق **مجازات**[2] به دنبال آن است که دشمن را از حمله منصرف کند، زیرا متوجه می‌شود که عواقب پرهزینه اقدام بیشتر از مزایای آن است. در این راهبرد دشمن باید متوجه این نکته شود که اگر دست به تهاجم زد به صورت تلافی‌جویانه مورد مجازات قرار خواهد گرفت. این راهبرد بازدارندگی را نیز می‌توان به دو دسته اقدامات کلی تقسیم کرد؛ از طرفی تلاش یک بازیگر برای بازدارندگی از تهاجمات یک بازیگر دیگر، و در طرف دیگر انجام مجموعه‌ای از اقدامات توسط کشورها که منجر به ایجاد اثر تجمعی در ایجاد بازدارندگی می‌شود. همان گونه که ذکر آن رفت، به دلیل عدم قطعیت امکان انتساب درست و شناسایی مهاجم، تهدید به مجازات و تلافی کارایی زیادی ندارد. با وجود این، این سازوکار همچنان به عنوان یکی از مهم‌ترین بخش‌های معادله بازدارندگی در فضای سایبر باقی خواهد ماند.

1. deterrence by denial
2. Deterrence by Punishment

نردبان پاسخ‌های این راهبرد بر اساس شدت حمله شامل اقدامات دیپلماتیک، اقتصادی، سایبری، قدرت فیزیکی و نیروی هسته‌ای خواهد بود. در این راستا استفاده آمریکا از کلیه روش‌های در دسترس در پاسخ به حمله سایبری، راهبرد ترکیبی پنتاگون نامگذاری شده است.

۳) بازدارندگی از طریق **وابستگی متقابل**[1] که بر بحث حل نشده در نظریه روابط بین‌الملل در مورد اینکه آیا وابستگی متقابل دولت‌ها به یکدیگر، تعارض بین آن ها را کاهش می‌دهد یا خیر، استوار است. یک نمونه مهم این است که استفاده از این سازوکار مستلزم درک مشترک همگان مبنی بر سودمندی استفاده از اینترنت و فضای مجازی برای ایشان است. در صورت رسیدن به چنین درکی، به احتمال زیاد به دنبال استفاده غیرصلح آمیز از این فضا نخواهند بود. بارزترین نمونه استفاده از این سازوکار در بازدارندگی، موضوع اختلافات سایبری آمریکا و چین است.(نای، ۲۰۱۷). در واقع این سازوکار بر اساس وابستگی متقابل کار می‌کند. برخی از وابستگی‌ها دو یا چند طرفه هستند، ولی برخی دیگر سیستمی بوده و در اثر اخلال در سیستم، منافع ایشان از دست خواهد رفت. در این حالت کشورها به دنبال ثبات سیستمی خواهند بود. البته این سازوکار برای همه کشورها کارایی ندارد. به عنوان مثال کشوری مانند کره شمالی را نمی‌توان با این سازوکار بازداشت.

۴) بازدارندگی از طریق **مشروعیت زدایی**[2] که بر ایجاد هنجارها و قوانینی برای رفتار دولت‌ها در فضای سایبری تمرکز می‌کند و در طول زمان به یک اصل کلی از خویشتن داری تبدیل می‌شود، هزینه‌های

1. Deterrence by Entanglement
2. Deterrence by De-legitimization

حیثیتی و خدشه دار شدن تصویر یک دولت ناشی از رفتار بد را، افزایش می‌دهد و فضای نبرد را محدود به صرف رزم نظامی می‌کند. در صورتی که بتوان با تصویب قوانین بین المللی، عملیات سایبری را به صورت تابو درآورد، آنگاه شکستن این تابوها برای کشورها هزینه خواهد داشت. در اصل بازدارندگی از این طریق، قدرت نرم کشورها را هدف قرار می‌دهد. هنجارها با گذشت زمان شکل می‌گیرند و هنجارسازی مراحلی دارد که در زمینه سایبر، در مراحل اولیه آن قرار داریم. در خصوص سازوکار هنجار، باید گفت که هنوز هنجارهای مؤثر بین المللی در این خصوص ایجاد نشده اند. هیچ سازمان بین المللی ای مسئولیتی در این خصوص نپذیرفته و در صورت بروز هرگونه حمله سایبری، اقدامات بین المللی هماهنگی صورت نخواهد پذیرفت(دهقانی، ۱۳۹۶). در رابطه با چهار راهبرد فوق نکته حائز اهمیت این است که مسئله عدم امکان انتساب می‌تواند مشکلاتی را برای سازوکارهای مجازات و هنجار(مشروعیت‌زدایی) ایجاد کند. ولی سازوکار های انکار و وابستگی متقابل نیازی به شناسایی و انتساب ندارند. نکته بعد آنکه استفاده از سازوکار انکار بیشتر می‌تواند گروه‌ها و دولت‌های ضعیف را از حمله منصرف کند چرا که دولت‌های قوی دارای آن چنان قدرت بالایی هستند که این روش‌ها قادر به بازداشتن آن‌ها نیستند. یکی از مهم ترین روش‌های ارتقای بازدارندگی سایبری خصوصاً میان قدرت‌های بزرگ سایبری، ایجاد، ارسال و جاسازی عوامل سایبری در درون زیرساخت‌های حیاتی کشور هدف است. با این اقدام، کشورها به دلیل نگرانی از احتمال بهره برداری طرف مقابل از این نرم افزارهای جاداده شده و تخریب زیرساخت‌ها و ایجاد بحران امنیت ملی، از اقدام تهاجمی در خصوص کشور مقابل بازداشته می‌شوند. در همین راستا، منابع آگاه در سازمان اطلاعات مرکزی آمریکا اعلام کرده‌اند که روسیه و چین اقدام

بـه جاسـازی قابلیت‌هـای سـایبری درون شـبکه بـرق آمریـکا نموده‌انـد کـه آن‌هـا را قـادر می‌سـازد در مواقـع مـورد نیـاز، کل شـبکه یـا بخش‌هایـی از آن را خامـوش نماینـد (دهقانـی، ۱۳۹۶). در نمـودار ۳، بـه صـورت خلاصـه، نظرات مختلـف اندیشـمندان در مـورد امـکان بازدارندگـی سـایبری ذکـر شـده اسـت.

نمودار ۴؛ انواع نظرات اندیشمندان در مورد امکان بازدارندگی سایبری

**توصیه‌هایی برای تامین امنیت و ایجاد بازدارندگی سایبری**

۱) وجود یک برگ برنده برای داشتن قدرت سایبری، یا راهبرد بازدارنده متمایز که بتواند مخاطره لازم را برای تهدیدکننده ایجاد نماید و همچنین اعلام اطلاعات این راهبرد در سطح ضرورت و به طور مناسب به تهدیدکننده، می‌تواند موفقیت بازدارندگی را تا حد زیادی تقویت نماید. شناختی که در تهدیدکننده درنتیجه تبادل اطلاعات و اعلان هشدارها از سوی بازدارنده به پشتوانه اقدامات معتبر بازدارنده صورت می‌گیرد، نشان می‌دهد که اساساً اطلاعات به خودی خود می‌تواند نه به صورت قطعی بلکه در سطح عقلانیت مشخصی از بازیگران بازدارنده باشد. یک بازیگر بازدارنده در صورتی که فاقد برگ برنده است می‌بایست با فریبِ تهدیدکننده زمان لازم را برای طراحی سازوکار جدید یا یک بازی جدید فراهم نماید(ملائی و همکاران، ۱۳۹۸).

۲)در حین انجام اقداماتی ایجابی برای ایجاد بازدارندگی، می‌بایست تدابیری نیز برای حفاظت لازم از زیرساخت‌هایی داخلی اتخاذ نمود. یکی از این موضوعات مهم، نگهداری یک نمونه از کلیه اطلاعات موجود در یک مکان امن است تا در صورت بروز حمله سایبری و از دست رفتن این اطلاعات، بتوان از اطلاعات پشتیبان استفاده نمود. موضوع مهم دیگر، برگشت پذیری است؛ به این معنا که در صورت هرگونه حمله سایبری و بروز خرابی، بتوانیم کل سیستم را به حالت اولیه برگردانیم(دهقانی،۱۳۹۶).

۳) بازیگران مدافع در فضای سایبری همیشه نیاز به ارزیابی اهداف و انگیزه‌های احتمالی یک دشمن (یعنی عوامل انسانی و زیرساخت‌های فنی) برای تطبیق با موارد مختلف دارند. بنابراین، پیامدهای مورد انتظار اقدامات خصمانه در فضای سایبری باید با در نظر گرفتن انگیزه‌های متمایز هر یک از بازیگران، به وضوح بیان شود. البته باید به این مسئله توجه کرد که در ارزیابی این انگیزه‌ها اولا،

برآوردهای دقیق برای بازدارندگی فقط برای دشمنان منطقی قابل انجام است. بازیگران فضای سایبری همیشه نمی‌توانند بازیگران غیرمنطقی را که اهمیت زیادی برای هزینه حملات سایبری خود و پیامدهای احتمالی آن قائل نیستند، بازدارند. ثانیا بازیگران تمایل دارند تصور کنند که دشمنان‌شان مسیرهای منطقی یکسان یا حداقل مشابهی برای رسیدن به نتیجه و تصمیم‌گیری دارند. آنها فرض می‌کنند که بازیگران اطلاعات کافی در مورد توانایی‌ها و انگیزه‌های طرف مقابل در اختیار دارند. این تصور نسبتاً عقلانی از رفتار بازیگران ممکن است لزوما مطابق با واقع نباشد و در نتیجه منجر به ایجاد سوگیری در تحلیل بازی و بازیگران شود. معیارهای عملیاتی و دقیق برای ارزیابی انگیزه‌ها و هزینه و منافع ادراک شده یک حمله برای ارزیابی درست موقعیت بسیار مهم است که اساس تئوری بازی‌ها و بازی‌های با حاصل جمع صفر را تشکیل می‌دهند. با این حال، هنگامی که درک دولت‌ها از شهرت خود یا نگرانی‌های آن‌ها در مورد عوامل نامشهود دیگر به معادله وارد می‌شود، حاشیه خطا گسترش می‌یابد و گاهی اوقات از محدوده واکنش‌های محاسبه شده فراتر می‌رود(بارک‌تُلقا، ۲۰۱۸).

**مسیرهای پیش روی بازدارندگی سایبری در آینده**

بعد از حمله سایبری آمریکا به استونی در سال ۲۰۰۷، شاهد افزایش روزافزون پژوهش و نگارش در حوزه بازدارندگی سایبری هستیم، که این روند در سال ۲۰۱۶ به اوج خود رسید؛ اما از این سال به بعد پژوهش و تفکر در مورد بازدارندگی سایبری به آرامی در بین محققان از رونق افتاده است. این مهم می‌تواند حداقل سه دلیل اصلی داشته باشد: ۱- همه چیز قبلاً گفته شده است؛ ۲- مفهوم بازدارندگی کاربست صحیحی در

فضای سایبری پیدا نکرده است و یا ۳- سایر مفاهیم راهبردی توجه بیشتری را به خود جلب می‌کنند. به احتمال زیاد شاهد ترکیبی از این دلایل هستیم، در نتیجه بعید است که این روند به این زودی‌ها معکوس شود. انتظار می‌رود که حوزه بازدارندگی سایبری در ادامه در چهار جهت منشعب شود که این جهات اگرچه متمایز و مجزا هستند اما متقابلاً یکدیگر را نفی نمی‌کنند(سوسانتو و اسمیتس، ۲۰۲۱):
۱) جهت اول به دنبال قرار دادن روزافزون بازدارندگی سایبری به عنوان عنصری در امنیت و منازعات بین المللی گسترده‌تر در دنیای پیچیدگی‌هاست. چالش اصلی آینده، تعریف بازدارندگی در فضای سایبری نیست، بلکه درک نقشی است که فناوری‌های دیجیتال در گستره وسیع‌تری از بازدارندگی در میان بازیگران مختلفِ رقیب ایفا می‌کنند. بازدارندگی بین حوزه‌ای[1] مفهوم جدیدی نیست، اما امروزه میزان توجه به آن در حال افزایش است. بازیگران راهبردی مدت‌هاست که قابلیت‌هایشان را با هم ترکیب کرده‌اند یا برخی حوزه‌ها را تغییر داده‌اند تا تهدیدهای قهرآمیز[2] ایجاد نمایند. از آنجایی که مجموعه وسیع‌تر و متنوع‌تری از ابزارهای موجود در روابط، انتخاب‌های راهبردی را پیچیده می‌کند، درک بهتر بازدارندگی بین حوزه‌ای برای تدوین یک راهبرد مؤثر امنیت ملی، به یک دارایی حیاتی تبدیل می‌شود.
۲) با توجه به ماهیت فنی حوزه سایبری، جهت دوم بر اثرات بازدارندگی در سطح عملیاتی و تاکتیکی متمرکز خواهد بود. در حال حاضر، مسائل عملی متعددی وجود دارد که مانع پژوهشگران و راهبردنگاران برای فهم و بررسی این مسیر می‌شود، از جمله: اسناد بسیار طبقه‌بندی شده، عدم دسترسی به اپراتورهای سایبری و نوپا بودن سازمان‌های سایبری نظامی موجود. با گذشت زمان، انتظار این است که این موانع از بین بروند تا جایی که

1. Cross-Domain Deterrence ،یا بازدارندگی بین حوزه‌ای، عبارت است از استفاده از قابلیت و ظرفیت یک حوزه برای دفع تهدیدات مهاجم در حوزه ای دیگر. مثل استفاده از نیروی نظامی هوایی برای پاسخ به اختلال سایبری از جانب دشمن
2. Coercive Threats

۳) جهت سوم به دنبال آن است که توجه را از بازدارندگی به شکل دیگری از برخورد قهرآمیز[1] معطوف نماید: یعنی اجبار اجبار به کنشی اطلاق می‌شود که حریف را متقاعد می‌کند که یک عمل را متوقف کند یا تغییر دهد. البته اجبار[2] به طور معمول امری دشوار در نظر گرفته می‌شود. هنگامی که بازیگری رفتار خود را تغییر می‌دهد، اغلب این تغییر رفتار هزینه‌هایی حیثیتی برای وی دارد. از این نظر، مزیتی که یک عملیات سایبری تهاجمی می‌تواند داشته باشد، این است که اگر اثرات این عملیات به صورت عمومی افشا نشده باشد، به این معنی است که طرف مجبور (یعنی مهاجم اولیه) می‌تواند پس از تهاجم و با هدف عدم تحمل هزینه حیثیتی مذکور، عقب نشینی نماید و منکر تاثیرپذیری از مدافع شود. به صورت کلی فرصت‌هایی برای معکوس کردن تاثیرات عملیات‌های سایبری و ایجاد تبعیت در مهاجم وجود دارد.

۴) جهت نهایی و چهارم مفاهیمی راهبردی را بررسی خواهد کرد که به دنبال مهار و جلوگیری کردن از تهاجم خصمانه در فضای سایبری است که از تفکر بازدارندگی سنتی متمایز است. درگیری مداوم[3] اولین گام در این مسیر است.[4] خطوط اولیه این مفهوم در مقاله ای در سال ۲۰۱۶ توسط ریچارد هارکنت و امیلی گلدمن[5] مطرح شد که در مورد یک محیط راهبردی پایدار در حمله[6] صحبت می‌کند

1. Coercion

در ادبیات روابط بین الملل، برخورد قهرآمیز اشاره به تحمیل هزینه‌هایی از جانب یک دولت نسبت به سایر بازیگران دولتی و غیردولتی دارد که هدف از آن جلوگیری از انجام برخی اقدامات (Deterrence) یا وادار ساختن برای انجام برخی رفتارها و افعال (Compellence) است

2. Compellence یا اجبار عبارت است از شکلی از برخورد قهرآمیز که تلاش دارد تا یک بازیگر مانند دولت، رفتارش را با تهدید به استفاده کامل یا محدود) از فشار نظامی تغییر دهد اجبار میتواند به عنوان راهبردی سیاسی-دیپلماتیک با هدف نفوذ بر اراده و ساختار انگیزشی دشمن) توصیف شود (https://en.wikipedia.org/wiki/Compellence)

3. Persistent Engagement

۴. تعامل مداوم مفهومی است که توسط فرماندهی سایبری ایالات متحده نیز در سند چشم انداز ۲۰۱۸ خود با عنوان دستیابی و حفظ برتری فضای سایبری» مورد توجه قرار گرفته است»

5. Richard Harknett and Emily Goldman
6. Offense-Persistent Strategic Environment

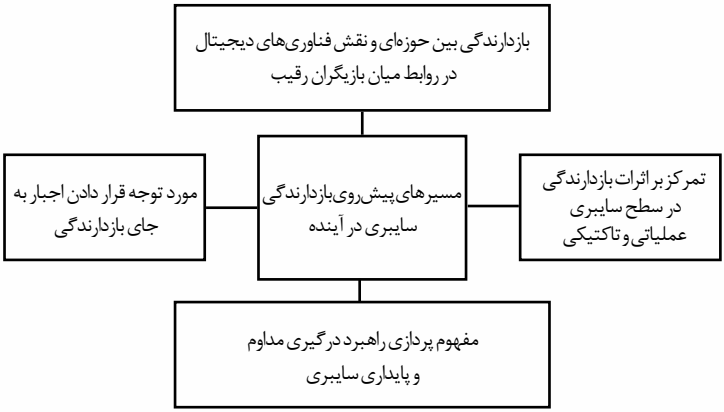
کـه در آن مقابلـه بیـن حملـه و دفـاع مسـتمر اسـت و دفـاع در تمـاس دائمـی بـا دشـمن اتفـاق می‌افتـد. علـت شـکل‌گیری اینمحیـط راهبـردی در ویژگی‌هـای رقابت‌پذیـری، بـه هم‌پیوسـتگی، کنش‌گـری مسـتمر، و محیـط در حـال تغییـر فضـای سـایبر قـرار دارد. فقـدان حالـت پایـدار در محیـط سـایبری بـه ایـن معنـی اسـت که حالـت دفاعـی پایـدار وجـود نـدارد. در عـوض، دفـاع یـک سـاخت پویـا نسـبت بـه فرصـت هـای تهاجمـی اسـت؛ دفـاع در هـر لحظـه خـاص در محـدوده پویـای فضـای سـایبری امـکان پذیـر اسـت و مـی توانـد در دوره‌هـای زمانـی از طریـق انطبـاق فعالانـه در محیـط حفـظ شـود. بـا ایـن حـال، دفـاع هرگـز نمی‌توانـد تعیین‌کننـده باشـد. پدافنـد می‌توانـد بـه موفقیـت تاکتیکـی و عملیاتـی دسـت یابـد، امـا حملـه ادامـه خواهـد داشـت و تمـاس و ارتبـاط بـا دشـمن ثابـت خواهـد مانـد. هارکنـت و مایـکل فیشـرکلر[1] یک سـال بعـد ایـن ایـده را پالایـش کـرده و اسـتدلال کردنـد کـه در یـک محیـط تمـاس دائمـی، اسـتراتژی مبتنـی بـر نـزاع و درگیـری مـداوم، مناسـب‌تر از مهـار عملیاتـی و واکنـش بـرای شـکل‌دهی بـه ویژگی‌هـای رفتـار قابـل قبـول و حفـظ و پیشـبرد منافـع ملـی ایـالات متحـده اسـت. چارچوبـی کـه هارکنـت و مایـکل فیشـرکلر بـرای ایـن محیـط پیشـنهاد می‌کننـد، پایـداری سـایبری[2] اسـت. . بـا اتخـاذ رویکـرد پایـداری سـایبری، کشـور مدافـع بـه دنبـال اسـتفاده از عملیـات، فعالیت‌هـا و اقدامـات سـایبری(در مقابـل تهدیـد بـه زور) بـرای ایجـاد مزیت‌هـای تاکتیکـی، عملیاتی و راهبـردی از طریـق تماس‌هـای عملیاتـی مـداوم و پایـدار(در مقابـل اجتنـاب از تمـاس) اسـت. بـه جـای یـک اسـتراتژی مبتنـی بـر تهدیـد، کـه بـر روی بازیگـر تهدیـد کننـده تمرکـز دارد، آنهـا یـک اسـتراتژی مبتنـی بـر قابلیت‌هـا پیشـنهاد می‌کننـد کـه آسـیب‌پذیری‌های مـا را پیش‌بینـی می‌کنـد و همزمـان از آسـیب‌پذیری‌های دیگـران اسـتفاده می‌کنـد (رُس، ۲۰۲۱).

1. Michael Fischerkeller
2. Cyber Persistence

زیربنای این دور شدن از تفکر بازدارندگی این باور است که تاکنون توجهی افراطی در ادبیات دانشگاهی به حمله و جنگ سایبری شده است درحالی که رفتار بازیگران در فضای مجازی ماهیت بسیار ظریف‌تری دارد. همان‌طور که هارکنت و اسمیت در مقاله‌ای در سال ۲۰۲۰ در مجله مطالعات استراتژیک نوشتند، آنچه پدیدار شده است، کمپین‌هایی[1] است متشکل از عملیات‌های سایبری مرتبط شده به یکدیگر با هدف خاص دستیابی به رهاوردهای راهبردی، بدون نیاز به حمله مسلحانه.همچنین به احتمال زیاد ما شاهد ظهور مفاهیم راهبردی دیگری، فراتر از درگیری مداوم خواهیم بود. می‌توان انتظار داشت که تحلیلگران کشورهای اروپایی ایده‌هایی را ارائه دهند که کاملاً در تضاد با تفکر آمریکایی است. از طرفی سیاست‌گذاران اروپایی مفهوم درگیری و نزاع مداوم را بیش از حد تهاجمی می‌دانند و از طرف دیگر، بیشتر سازمان‌های سایبری نظامی اروپایی قادر نیستند، ظرفیت‌های عملیاتی خود را به‌قدری افزایش دهند که بتوانند «به‌طور یکپارچه، جهانی و پیوسته»، به‌عنوان نیازهای راهبرد درگیری مداوم، حرکت کنند. با درک این محدودیت‌ها، کشورهای عضو اتحادیه اروپا باید این خلاء راهبردی را با تفکر مفهومی خلاق پر کنند. در ادامه و در نمودار ۴، مسیرهای پیش‌روی بازدارندگی سایبری در آینده به صورت اجمالی ترسیم شده است.

1. Campaigns

نمودار ۵؛ مسیرهای پیش‌روی بازدارندگی سایبری در آینده



# نتیجه گیری

## نتیجه‌گیری

هـدف گـزارش حاضـر، گـردآوری و تنظیـم نکاتـی در رابطـه بـا مفهـوم بازدارندگـی سـایبری و مفاهیـم پیرامونـی آن ماننـد قـدرت، حملـه و جنـگ و دفـاع سـایبری بـود. مشـخص شـد کـه راهبـرد بازدارندگـی، یکـی از مهم‌تریـن راهبردهـای تامیـن امنیـت در روابـط میـان بازیگـران و خصوصـا میـان دولت‌هـای مختلـف اسـت. بنابرایـن بازدارندگـی می‌توانـد در تامیـن امنیـت فضای‌سـایبری یـک کشـور موثـر واقـع گـردد؛ فضایـی کـه امـروزه با گسـترش فناوری‌هـای اطلاعـات و ارتباطـات بـه محـل زیسـت و تعامـلات اجتماعـی شـهروندان کشـورها و در نتیجـه بازتولیـد نظام‌هـای اجتماعـی در ایـن بسـتر تبدیـل گردیـده اسـت. همانگونـه کـه ذکر شـد، میزان جنـگ و تهاجم‌هـا میان بازیگـران مختلـف در فضای‌سـایبری بـه علـت ویژگی‌هـای ماهـوی ایـن فضـا شـدت و سـهولت بیشـتری از فضـای واقعـی دارد. بنابرایـن در گـزارش حاضـر، پـس از بررسـی مفاهیمـی چـون قـدرت سـایبری، جنـگ و حملـه سـایبری و دفـاع سـایبری و ذکـر تفاوت‌هـای ماهـوی منازعـات میـان بازیگـران در فضـای واقعـی و فضـای مجـازی، بـه بررسـی ابعـاد مفهـوم بازدارندگـی پرداختـه شـد. بازدارندگـی بـه معنـای منصـرف کـردن کسـی از انجـام کاری بـا ایجـاد ایـن بـاور در اوسـت کـه هزینه‌هـای ایـن کار از منافـع مـورد انتظـارش فراتـر خواهد رفـت. سـه مولفـه اساسـی بازدارندگـی سـایبری نیـز عبـارت اسـت از سیسـتم

دفاعی مستحکم برای محافظت از زیرساخت‌ها، توانایی انتساب و شناسایی مهاجم، تمایل و توانمندی تلافی علیه هر حمله‌ای. در میان نظرات متفاوتی که اندیشمندان حوزه امنیت در رابطه با بازدارندگی سایبری و امکان و کیفیت آن ارائه کرده اند، گروهی معتقدند با درک تفاوت‌های ماهوی فضای سایبری و واقعی، می‌توان راهبردهای چهارگانه ای را ارائه کرد: بازدارندگی از طریق انکار، مجازات، وابستگی متقابل و مشروعیت‌زدایی. نکته حائز اهمیت این است که تحقیقات و تحلیل‌های زیادی در مورد تفاوت‌های کلیدی و چگونگی ایجاد یک موقعیت بازدارندگی معتبر در فضای سایبری علیه بازیگران دولتی و غیردولتی، هکریست‌ها و تروریست‌های سایبری انجام شده است که در نتیجه، شیوه‌های بسیار کامل و استانداردی ایجاد شده است. با این حال تعداد حوادث سایبری کاهش نیافته است. به نظر می‌رسد که نظریه‌های بازدارندگی توصیه شده آن‌طور که در زندگی واقعی طراحی شده‌اند، در فضای سایبر اثرگذار نیستند. اما با این وجود در ارزیابی کلی، می‌توان گفت درحالی که هیچ یک از این سازوکارها کامل نیستند، ولی در صورت اتخاذ ترکیبی از این راهبردها، در کنار هم می‌توانند حملات سایبری را کاهش داده و محیطی امن‌تر ایجاد کنند. در نهایت، چهار مسیر پیش بینی شده برای ادامه مطالعه بازدارندگی در آینده نیز عبارت اند از بررسی نقش فناوری‌های دیجیتال در روابط میان بازیگران مختلف رقیب در چارچوب بازدارندگی بین حوزه‌ای، تمرکز بر اثرات بازدارندگی سایبری در سطح عملیاتی و تاکتیکی، مورد توجه قرار دادن اجبار به جای بازدارندگی، مفهوم پردازی راهبرد درگیری مداوم و پایدار سایبری.

# منابع

• فیروزآبادی، سید ابوالحسن؛ آزادی احمدآبادی، جواد (۱۳۹۹): تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران.نشریه علمی دانش سیاسی، ۱۶(۲) ۵۶۳-۵۹۸.
• آزادی احمد آبادی، جواد (۱۳۹۷): امنیت سایبری یا امنیت فضای مجازی؟، تاملات رشد، ۱ (۱): ۱۶۴-۱۶۸.
• دهقانی، علی‌اصغر (۱۳۹۶): بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا، فصلنامه رهیافت های سیاسی-بین المللی، ۸ (۴): ۱۲۱-۱۴۷.
• زابلی زاده، اردشیر؛ وهاب پور، پیمان، (۱۳۹۷): قدرت بازدارندگی در فضای سایبر؛ رسانه و فرهنگ، ۸ (۱): ۴۷-۷۴.
• ملائی، علی؛ کارگری، مهرداد؛ شیخ محمدی، مجید، اکرمی زاده، علی، (۱۳۹۸): مدل بازدارندگی در فضای سایبر مبتنی بر گراف حمله باورهای بیزی با استفاده از ترجیحات مخاطره آفرینی، پدافند الکترونیکی و سایبری، ۷ (۱): ۲۵-۳۸.
• ملائی، علی؛ کارگری، مهرداد؛ خرداشادی زاده، محمدرضا، (۱۳۹۷): الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی ها، فصلنامه امنیت ملی، ۸ (۲۹): ۱۴۱-۱۷۲.
• مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۷۵)، تئوری بازدارندگی (نظریات کلان منازعه).

- Nye, Joseph S. 2017: Deterrence and Dissuasion in Cyberspace. International Security, President and Fellows of Harvard College and the Massachusetts Institute of Technology, 44-71.
- Soesanto, Stefan. Smeets, Max. (2021): Cyber Deterrence: The Past, Present, and Future, NL ARMS Netherlands Annual Review of Military Studies 2020, 385-400. https://doi.org/10.1007/978-94-6265-419-8_20
- Burak Tolga, Ihsan. (2018): Principles of Cyber Deterrence and theChallenges in Developing a Credible Cyber Deterrence Posture. CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). www.ccdcoe.org / publications@ccdcoe.org
- Ross, Maj Caeron. (2021): Is It Time to Forget about Cyber Deterrence?, AIR & SPACE POWER JOURNAL, 69-73.
- https://fa.wikipedia.org/wiki/%D8%B9%D9%85%D9%82_%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%DA%98%DB%8C%DA%A9
- https://en.wikipedia.org/wiki/Compellence
- http://www.irdiplomacy.ir/fa/person/549/جوزف_نای


csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir