DOI: 10.22034/ISJ.2022.299267.1562

International Studies Journal (ISJ)
Vol. 18, No. 3 (71), Winter 2021
Reseived Date: 2021/9/4
Accept Date: 2021/12/21
Article Type: Original Research
PP: 187-206

فصلنامه مطالعات بین‌المللی
سال۱۸، شماره۳(۷۱)، زمستان۱۴۰۰
تاریخ دریافت: ۱۴۰۰/۶/۱۳
تاریخ پذیرش: ۱۴۰۰/۹/۳۰
نوع مقاله: علمی- پژوهشی
صفحات: ۲۰۶-۱۸۷

شیوه‌های نوین تقابل میان جمهوری اسلامی ایران و آمریکا در فضای سایبر (۲۰۲۰-۲۰۱۰)*

رضا سلگی[1]- دکتر حسن خداوردی[2]
دکتر زهره پوستین‌چی[3]

چکیده

امروزه بستر ارتباطی اینترنت و فضای سایبر، ماهیت تعامل میان جمهوری اسلامی ایران و ایالات متحده آمریکا را دگرگون نموده و شیوه‌های نوینی از کنش و واکنش در روابط آنها را به ارمغان آورده است. هدف از این پژوهش این است تا با استفاده از روش توصیفی- تحلیلی جهت آزمون فرضیه و روش کتابخانه‌ای و فیش‌برداری برای گردآوری داده‌ها و اطلاعات، در کنار بکارگیری از گزاره‌های نظریه قدرت اجبار، به این سوال پاسخ دهد که شیوه‌های نوین تقابل میان ایران و آمریکا در فضای سایبر چه می‌باشد؟ نتایج حاصل از این پژوهش به این مورد اشاره می‌کند که تفاوت رویکردهای آمریکا و ایران در خصوص مسائل منطقه‌ای و حل نشدن مشکلات فی مابین و افزایش تحریم‌های بین‌المللی علیه ایران و از همه مهم‌تر، خروج آمریکا از توافق برجام و ترور فرمانده سپاه قدس ایران باعث شده است تا عرصه سایبر بیش از پیش به یکی از عرصه‌های برجسته برای تقابل میان این دو کشور تبدیل شود. به طوری که هر یک با توجه به سطح توانمندی و مقدورات خود در حوزه فناوری‌های سایبری و بکارگیری انواع روش‌ها و ابزارها به نحوی از این توانمندی به عنوان ابزار اعمال قدرت و اجبار علیه دیگری و تحمیل اراده خود بهره‌برداری نموده‌اند، تا بتوانند طرف مقابل را به تغییر رفتار و مواضع و یا پذیرش خواسته‌های خود مجبور نماید.

کلیدواژگان: ایران، آمریکا، اینترنت، فضای سایبر، شیوه‌های نوین تقابل، حملات سایبری

* این مقاله برگرفته از رساله دکتری روابط بین‌الملل رضا سلگی با عنوان «نقش تکنولوژی سایبر در شیوه‌های نوین تقابل میان جمهوری اسلامی ایران و ایالات متحده آمریکا (۲۰۲۰-۲۰۱۰)» با راهنمایی دکتر حسن خداوردی است.

[1] دانشجوی دکتری علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
[2] نویسنده مسئول، استادیار گروه علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران. / ایمیل: h_khodaverdi@azad.ac.ir
[3] استادیار گروه علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

Article Link: https://www.isjq.ir/article_148495.html

مقدمه

در سال‌های اخیر، فضای سایبر به‌طور فزاینده‌ای به عنوان حوزه درگیری بین قدرت‌های پیش‌رو جهانی و منطقه‌ای ظاهر شده است. به طوری که فعالیت‌های مخرب سایبری به صورت فردی و یا تحت حمایت دولت‌ها، نسل جدیدی از تهدیدات را در مقیاس جهانی، فراروی امنیت ملی دولت‌ها ایجاد کرده است. تامین امنیت فیزیکی و سایبری بخش‌های زیرساخت‌های حیاتی یک کشور که خدمات ضروری برای زندگی و کار را در محدوده پارادایم‌های امنیتی در حال تکامل ارائه می‌دهند، بسیار مهم شده است. اکنون فضای مجازی به عنوان یک میدان مبارزه جدید در سطح دولتی شناخته می‌شود. از این‌رو، سرمایه‌گذاری در دفاع سایبری و تقویت ظرفیت‌های حمله در رقابت مداوم و جنگ قدرت در سیستم بین‌المللی نیز افزایش یافته است که به نوبه خود بر ادراک تهدید متقابل کشورها نسبت به هم، تأثیر بسزایی داشته است.

فهم و شناخت جامع و دقیق فضای سایبر و شیوه‌های نوین کنش‌گری در این فضا، نیازمند داشتن دانش کافی و پایش و ارزیابی مستمر و دقیق توانمندی‌های سایبری خود و دیگر رقبا می‌باشد. زیرا در غیر این صورت، اقدامات تهاجمی و یا دفاعی نسنجیده در این حوزه می‌تواند تبعات جبران‌ناپذیری را برای زیرساخت‌های حیاتی کشورها به همراه داشته باشد. نمونه بارز آن را می‌توان در تقابل میان آمریکا و ایران در عرصه فضای سایبر در طول کمتر از دو دهه گذشته به وضوح مشاهده نمود. با توجه به اهمیت موضوع، این پژوهش به‌دنبال پاسخ‌گویی به این پرسش می‌باشد که شیوه‌های نوین تقابل میان جمهوری اسلامی ایران و آمریکا در فضای سایبر چه می‌باشد؟ در ارتباط با سوال پژوهش این فرضیه مطرح می‌گردد که ایالات متحده آمریکا و جمهوری اسلامی ایران، با استفاده از تمامی قابلیت‌ها و مقدورات خود در حوزه فناوری‌های نوین سایبری در کنار اتخاذ جدیدترین روش‌ها و تاکتیک‌ها و بکارگیری جدیدترین و مدرن‌ترین ابزارهای مخرب سایبری به نحوی از این توانمندی به عنوان ابزار اعمال قدرت و اجبار بر علیه دیگری و تحمیل اراده خود بهره‌برداری نموده‌اند، تا بتوانند طرف مقابل را به تغییر رفتار و مواضع و یا پذیرش خواسته‌های خود مجبور نماید. هدف از پژوهش آن است تا با استفاده از روش توصیفی-تحلیلی جهت آزمون فرضیه و روش کتابخانه‌ای و فیش‌برداری برای گردآوری داده‌ها و اطلاعات، در کنار بکارگیری از مولفه‌ها و گزاره‌های نظریه «قدرت اجبار» در راستای آزمون فرضیه گام بردارد.

۱- پیشینه موضوع

کامیسکی، در مقاله‌ای تحت عنوان « عملیات بازی‌های المپیک؛ خرابکاری سایبری به عنوان ابزار جامعه اطلاعاتی آمریکا برای خنثی‌سازی برنامه هسته‌ای ایران»، به تشریح عملیات سایبری آمریکا علیه ایران با رمز «بازی‌های المپیک» و نحوه استفاده از روش‌ها و منابع اطلاعاتی می‌پردازد

که از سال ۲۰۰۶ و تحت رهبری دولت جورج دبلیو بوش آغاز شده و در ابتدا توان هسته‌ای ایران و به تدریج دیگر زیرساخت‌های حیاتی جمهوری اسلامی ایران را مورد هدف قرار داده است (Kaminski, 2020). فیکسلر، در تحقیقی با عنوان «تهدید سایبری از ایران پس از مرگ سلیمانی»، به بررسی اقدامات تلافی‌جویانه و حملات سایبری ایران علیه آمریکا پس از ترور ژنرال قاسم سلیمانی به دست ارتش آمریکا می‌پردازد. این مقاله بسیار مختصر و موردی به تعدادی از اقدامات ایران پس از این اقدام اشاره می‌نماید (Fixler, 2020). آیزنستاد، در پژوهشی تحت عنوان «طولانی شدن سایه سایبری ایران»، به واکنش تلافی‌جویانه سایبری ایران بر علیه مخالفان خود می‌پردازد. و تاکید می‌کند که سایبر به عنوان یک سلاح انتخابی ایران، برای برخورد با مخالفان داخلی و دشمنان خارجی، با یک روند رو به رشدی در حال توسعه می‌باشد (Eisenstadt, 2016). موحدیان، در کتاب خود تحت عنوان «سایبر دیپلماسی آمریکا در قبال ایران در دوره ریاست جمهوری باراک اوباما» به بررسی دیپلماسی سایبری آمریکا در قبال ایران پرداخته و نحوه استفاده دولت‌های جرج بوش پسر و باراک اوباما، از شبکه‌های اجتماعی و سایر ظرفیت‌های فضای مجازی برای تاثیرگذاری بر کاربران ایرانی اینترنت را تشریح نموده است (موحدیان، ۱۳۹۹)؛(Movahedian, 2020).

۲- مبانی نظری: قدرت اجبار

دیوید گامپرت[۱] و هانس بیننداِیک[۲] در پروژه مطالعاتی اندیشکده سیاست‌گذاری رند[۳] و در چارچوب پایه‌ریزی بسترهای نظری اقدامات دولت آمریکا، و نیز جهت تهیه گزارش‌های دفاعی ارتش آمریکا، در پی ایجاد موازنه میان محدودیت‌ها و فرصت‌ها، مفهوم «قدرت اجبار» و ابزارهای آن را به عنوان رویکردهای جایگزین جهت تامین منافع و ارتقاء «امنیت سخت» آمریکا ارائه کرده‌اند (علیخانی، ۱۳۹۹: ۶۵-۶۶)؛(Alikhani, 2020: 65-66).

قدرت اجبار، نوع دوم از سه نوع روش اعمال قدرت و اقتدار علیه مخالفان و دشمنان است. اگر «قدرت سخت»، نوع اول از سه‌گانه و «قدرت نرم» از نوع سوم آن باشد، بی‌گمان نوع دومی از قدرت است که در اصطلاح از آن به «قدرت اجبار» یاد می‌شود. قدرت اجبار، اجرای روش‌ها و ابزارهایی است تا دشمن، وادار به تغییر رفتار و پذیرش موضع مناسب شود. «از نظر گامپرت و بیننداِیک، عملیات سایبری تهاجمی[۴] یکی از مصادیق قدرت اجبار می‌باشد. گسترش تاکتیکی جنگ سایبری به معنی تخریب سیستم‌های کامپیوتری کشور هدف، یکی از ابزارهای پر ریسک

---

۱. معاون و سپس کفیل اطلاعات ملی آمریکا در دوره باراک اوباما (۲۰۱۰)

۲. خدمت در شورای امنیت ملی آمریکا و متخصص امنیتی و دفاعی

3. RAND Corporation

4. Offensive Cyber Operations

اجبار است. البته باید در نظر گرفته که حمله سایبری می‌تواند مقدمه یک حمله فیزیکی نیز باشد (Gompert and Binnendijk, 2016: 14-16). گامپرت و بیندایک در بررسی عملیات سایبری تهاجمی به عنوان یکی از ابزارهای قدرت اجبار به این نتیجه رسیده‌اند که این ابزار با وجود اینکه از جلب حمایت بین‌المللی پایین و هزینه‌ها و ریسک‌های بالایی می‌باشد، اما دارای میزان اثرگذاری نیز بالایی می‌باشد (Gompert and Binnendijk, 2016: 32).

۳- سایبر و شیوه‌های نوین کنش‌گری در روابط کشورها

امروزه جوامع مدرن بسیار بیشتر از هر زمان دیگری به فناوری‌های پیچیده و پرکاربرد مبتنی بر اینترنت وابسته هستند. این دولت‌ها استراتژی‌ها را تبیین نموده، ساختارهای نهادی ویژه‌ای ایجاد کرده و نیروهای مسلح خود را اصلاح می‌کنند تا دفاع سایبری و ظرفیت حمله خود را در مقابل دشمنان خود بدون توجه به قدرت اقتصادی، ظرفیت نظامی یا سطح توسعه فناوری خود بهبود بخشند. «با گسترش سریع فناوری در قرن بیست و یکم، جامعه به شدت به زیرساخت‌های دیجیتال وابسته شده است. این وابستگی نیز به موازات حوزه پنجم جنگ، یعنی سایبر تکامل یافته است (Goel, 2020: 90). « پتانسیل حملات سایبری برای عبور به حوزه فیزیکی بارها توسط هکرها اثبات شده است. این حملات باعث ایجاد وحشت عمومی گسترده در یک کشور می‌شوند و لذا توجیه کافی برای تلافی یک اقدام سایبری را فراهم می‌کند. پاسخ به این حمله می‌تواند شامل اقدامات تهاجمی بازدارنده سایبری علاوه بر عملیات نظامی متعارف باشد»(Epps, 2021: 7).

٤- تقابل آمریکا و ایران در فضای سایبر

تنش فزاینده میان ایالات متحده آمریکا و ایران پس از سال ۱۹۷۹ به اصلی‌ترین مشخصه روابط دو کشور در چند سال اخیر تبدیل شده است. در چارچوب اجرای سیاست‌های امنیتی آمریکا در جهت مبارزه با تروریسم پس از ۱۱ سپتامبر، لشگرکشی این کشور به عراق و افغانستان و عدم توجه به منافع منطقه‌ای ایران و از همه مهم‌تر، اعلام ایران به عنوان محور شرارت از سوی آمریکا، همگی نشانه‌هایی بوده است مبنی بر اینکه روابط ایران و آمریکا در آینده پرتنش‌تر خواهد شد.

با ظهور انقلاب تکنولوژی ارتباطات و اطلاعات « اینترنت فضای جدیدی از رقابت، دشمنی و جنگ را میان این دو کشور ایجاد نموده است این محیط به سرعت در حال تغییر است. این تغییرات و سیال بودن فضای سایبر، چالش بسیار بزرگی را برای این دو کشور در قبال یکدیگر به وجود آورده است»(صانعیان، ۱۳۹۸: ۲۰۷-۲۰۸)؛(Saneian, 2019: 207-208).

اگرچه اختلاف رویکردها و فعالیت‌های منطقه‌ای دو کشور همواره باعث تنش میان آمریکا و ایران بوده است، اما عامل اصلی تنش‌ها، اجرای برنامه هسته‌ای توسط جمهوری اسلامی ایران بوده

است. از این‌رو، آمریکا با فشارهای چند بُعدی و به ویژه اقتصادی، همواره سعی در کنترل ایران داشته است. تقابل این دو کشور در فضای سایبری به موازات مذاکرات این دو کشور در حوزه هسته‌ای به خوبی نشان داده است که درک تهدید در حال رشد بین دو کشور، تنها به ابعاد آن در دنیای فیزیکی محدود نمی‌شود. حتی با وجود آغاز فرآیند گفتگوهای برنامه جامع اقدام مشترک[1] (برجام) بین دو کشور در دوره ریاست جمهوری اوباما، هم آمریکا و هم ایران با اقدامات متعدد فیزیکی و سایبری در سیاست‌های منطقه‌ای خود، برداشت‌های خود را از یکدیگر آشکار کرده‌اند که این امر نشان از تدام بحران اعتماد بین طرفین بوده است (Bulut, 2021: 185-186).

٤-١- ابعاد اقدامات سایبری آمریکا بر علیه ایران

دلیل اصلی پیگیری دقیق تحولات فضای مجازی و تلاش برای درگیر شدن در این فرآیندها، جنگ قدرت و رقابت نظامی میان دولت‌ها در محدوده الگوی رئالیستی است. امروزه دولت‌ها، نظیر ایالات متحده آمریکا، برنامه‌های خود را برای توسعه یک حمله سایبری مؤثر و ظرفیت دفاعی با استفاده از پیشرفت‌های مبتنی بر فناوری شبکه بیش از پیش تسریع کرده‌اند (Burak & Soner, 2022: 274).

به گزارش شورای روابط خارجی آمریکا و مرکز راهبردی و مطالعات بین‌المللی[2] بیش از ۲۵۰ حمله سایبری تحت حمایت دولت ایالات متحده در دوره زمانی از ۲۰۰۵ تا ۲۰۱۸ شناسایی شده است (Tikk, 2019:25).

تأسیس فرماندهی سایبری آمریکا در سال ۲۰۰۹ و کسب مقام فرماندهی عملیاتی مستقل در ماه می ۲۰۱۸ (تا آن زمان جزئی از فرماندهی راهبردی بود)، اهمیت فضای سایبری را برای پنتاگون نشان می‌دهد. در استراتژی ملی سایبری آمریکا منتشر شده در سپتامبر ۲۰۱۸، هدف، شناسایی، مقابله، منحرف کردن، تحقیر و بازدارندگی رفتارهایی در فضای سایبری است که بی‌ثبات کننده و مغایر با منافع ملی ایالات متحده است، یعنی دست‌یابی ایالات متحده به تسلط و برتری در فضای مجازی. اگر این استراتژی به طور کامل اجرا شود، شامل اقداماتی علیه برخی بازیگران در فضای سایبری خواهد بود، که این مورد علیه ایران به اتهام سرنگونی پهپاد آمریکایی در دریای عمان به اجرا در آمد. اسناد راهبردی ایالات متحده بر حق اقدامات متقابل و دفاع از خود در صورت حمله سایبری تأکید دارد. نگرش ایالات متحده نسبت به فضای سایبری بیشتر تدافعی بود و هدف اصلی آن بازدارندگی مهاجمان بالقوه بوده است. ایالات متحده معتقد است که درک توانایی‌های تهاجمی ایالات متحده توسط دشمنان این کشور می‌تواند آنها را از حمله کردن به آمریکا منصرف کند (Vuletic et al, 2021: 78-79).

---

[1]. Joint Comprehensive Plan of Action

[2]. Strategic and International Studies (CSIS)

فعالیت‌های سایبری آمریکا علیه ایران، به طور گسترده‌ای در یک کمپین مخفی با اسم رمز بازی‌های المپیک[1] در سال ۲۰۰۶ و تحت رهبری دولت جورج دبلیو بوش آغاز شد، که در ابتدا توان هسته‌ای ایران را مورد هدف قرار داده بود. اوباما رئیس‌جمهور بعدی آمریکا نیز کمپین بازی‌های المپیک را توسعه داد تا شامل استفاده از سلاح‌های سایبری تهاجمی علیه تأسیسات غنی-سازی هسته‌ای ایران نیز بشود (Kaminski, 2020: 64-70). «اولین اشاره به کمپین بازی‌های المپیک توسط «دیوید سنگر» بود که مدعی شد این عملیات اقدام مشترک آمریکا و اسرائیل است که به منظور برهم زدن برنامه هسته‌ای ایران به اجرا در آمد. این عملیات که بعدها به نام «نیترو زئوس» شناخته شد در صورت شکست مذاکرات هسته‌ای، یک طرح اضطراری را آماده اجرا داشت. این برنامه برای یک عملیات سایبری تهاجمی حمله به شبکه‌های ایران با هدف از کار انداختن رایانه‌ها در تأسیسات هسته‌ای فردو، و همچنین از کار انداختن پدافند هوایی، ارتباطات و شبکه‌های برق ایران برنامه‌ریزی گردید» (Baezner, 2019: 12).

گزارش‌ها نشان می‌دهد حملات بدافزار استاکس‌نت بر علیه تاسیسات اتمی ایران در سال ۲۰۱۰، تنها بخش کوچکی از پروژه بزرگ نیتروزئوس بوده است. بر اساس این پروژه بود که متخصصین امور دفاعی و امنیتی آمریکا، آسیب‌پذیری ایران را این‌گونه بیان کردند: «ایالات متحده می‌تواند کل زیرساخت‌های ایران را بدون رها کردن حتی یک بمب نابود کند» (لرستانی،۱۳۹۷:۱۵۰)؛ (Lorestani, 2019: 150).

به دلیل گستردگی عملکرد، استفاده جسورانه و عنصر غافلگیری، تأثیر استاکس‌نت قابل توجه بود. نه تنها در مورد خود برنامه هسته‌ای، بلکه در مورد روابط بین‌الملل، توسعه استراتژی‌ها و در کل حوزه امنیت سایبری. «اگرچه تا سال ۲۰۱۰ حملات سایبری با توانایی فنی بالاتر وجود داشت، اما تا آن زمان هیچ حمله سایبری به این وسعت نرسیده بود. بر اساس گزارش‌ها، این حمله، یک پنجم سانتریفیوژهای تأسیسات اتمی نطنز را نابود کرد و به طور قابل توجهی سرعت برنامه هسته‌ای ایران را کاهش داد» (Craig and Valeriano, 2016: 150).

به تدریج ویروس‌ها یکی پس از دیگری، تاسیسات حیاتی ایران را آماج حملات خود قرار داده‌اند. «در سپتامبر ۲۰۱۱، تهدید دیگری به نام Duqu کشف شد این ویروس در سال ۲۰۱۵ نیز با ورژن Duqu2 منتشر گردید که وظیفه آن حمله به رایانه‌های هتل‌ها، شرکت‌ها و افراد شرکت کننده در مذاکرات هسته‌ای ایران در سوئیس و اتریش بوده است. تجزیه و تحلیل شرکت سیمانتک نشان داد که Duqu تقریباً مشابه استاکس‌نت است، فقط هدف متفاوتی دارد. تفاوت آن دو در توانایی Duqu در انتقال داده‌ها از راه دور به جای خرابکاری در سیستم‌های کنترل صنعتی مشابه استاکس

[1]. Operation Olympic Games

نت بوده است» (Utinkova, 2021: 26).

عامل تهدید دیگری بنام Flame با استفاده از یک ابزار مخرب در می ۲۰۱۲ کشف شد. «این بدافزار بیشتر در کشورهای خاورمیانه گسترش یافت و ایران از جمله کشورهایی بود که بیشترین آسیب را دید. الکساندر گوستف، کارشناس ارشد امنیت در آزمایشگاه کسپرسکی گفته است: «بدافزار فلیم، ۲۰ برابر پیچیده‌تر از استاکس نت بوده است». اندکی پس از کشف Flame، یک حمله سایبری دیگری با نام با نام «گاوس» در کشورهای خاورمیانه به خصوص ایران عملیاتی شد. ویژگی منحصر به فرد گاوس، توانایی سرقت اطلاعات بانکی بود. بررسی‌های تخصصی نشان داد که بین استاکس‌نت، دوکو، فلیم و گاوس ارتباط نزدیکی وجود دارد، به طوری که به نظر می‌رسید همه این بدافزارها از طرف یک توسعه دهنده مشترک پشتیبانی می‌شوند» (Baezner, 2019: 12).

فعالیت یک عامل تهدید دیگر در ایران به نام «عملیات پارلمان» در سال ۲۰۱۷ آشکار شد. «اهداف این عامل تهدید، عمدتاً دارای ارزش استراتژیک بالایی بودند، مانند دولت‌ها، وزارتخانه‌ها، مؤسسات، رسانه‌ها و شرکت‌ها. در اکتبر ۲۰۱۸ نیز یعنی سه سال پس از آخرین حمله سایبری مرتبط با عملیات المپیک، اطلاعاتی در مورد نسخه جدیدی از استاکس‌نت در ایران توسط رئیس سازمان دفاع غیر عامل ایران، غلامرضا جلالی اعلام شد. استاکس‌نت۲، آخرین حمله سایبری شناخته شده بود که ظاهراً به استاکس‌نت اصلی و بازی‌های المپیک مرتبط بوده است» (Utinkova, 2021: 28).

اگرچه از سال ۲۰۱۸ هیچ اثری از حملات سایبری مرتبط با استاکس‌نت گزارش نگردید، اما با شروع دوباره تنش‌ها میان جمهوری اسلامی ایران و ایالات متحده آمریکا، در دوران دولت ترامپ، به ویژه پس از اعلام خروج آمریکا از برجام در ۸ می ۲۰۱۸، ایران شاهد افزایش حملات سایبری بود. مهم‌ترین تشدید تنش در آوریل ۲۰۱۹ اتفاق افتاد، زمانی که ایالات متحده، سپاه پاسداران انقلاب اسلامی ایران را که شاخه‌ای از نیروهای مسلح ایران است، در فهرست سازمان‌های تروریستی قرار داد (Barnes & Gibbons, 2019). «در ژوئن سال ۲۰۱۹، ایالات متحده پس از سرنگونی یک فروند هواپیمای بدون سرنشین خود در نزدیکی تنگه هرمز، یک حمله سایبری علیه ایران انجام داد. این حمله، یک پایگاه داده سپاه پاسداران انقلاب اسلامی را که به ادعای آمریکا برای برنامه‌ریزی حملات علیه تانکرها در خلیج فارس استفاده می‌شد، پاکسازی کامل کرد» (Katzman, 2020: 3).

افزایش تنش‌ها میان جمهوری اسلامی ایران و ایالات متحده آمریکا از ۱۴ سپتامبر ۲۰۱۹ مجددا اوج گرفت. زمانی که تاسیسات نفتی خریص و بقیق عربستان سعودی در حمله‌ای سایبری منتسب به ایران که باعث افزایش بی‌سابقه قیمت نفت شد، آسیب دیدند (Utinkova, 2021: 29).

در بین این حملات سایبری بزرگ علیه ایران که اغلب به یک رویداد ژئوپلیتیکی مرتبط هستند، حملات سایبری‌ای با اهمیت کمتر نیز رخ داده است. یکی از نمونه‌های آن، مجموعه‌ای از حملات

به بنادر ایران، سازمان‌های مرتبط با آن و سایر سازمان‌های دولتی است که بین ماه مه و اکتبر ۲۰۲۰ آشکار شد. علاوه بر این، در نوامبر ۲۰۲۰، ایالات متحده حملات سایبری دیگری را علیه گروه هکر ایرانی مرتبط با سپاه پاسداران انقلاب اسلامی، هدف قرار داد. مدیر اطلاعات ملی، «جان رتکلیف»، اظهار داشت که ایران با ارسال ایمیل‌های جعلی و پیام‌های متنی با هدف تحقیر دونالد ترامپ، تلاش کرد بر انتخابات ریاست‌جمهوری آمریکا تأثیر بگذارد. به همین دلیل، ایالات متحده حملات سایبری تهاجمی را با هدف توقف تبلیغات پیش از انتخابات آمریکا انجام داد و ابزارها، شبکه‌ها و باج‌افزارهای ایرانی را آفلاین کرد. این رویکرد پیشگیرانه جدید توسط ژنرال پل ناکاسون، فرمانده فرماندهی سایبری ایالات متحده و مدیر آژانس امنیت ملی، به عنوان یک «تعامل مداوم» و «دفاع از جلو» توصیف شد که به «عمق رفتن در شبکه‌های رایانه‌ای دشمنان» اشاره دارد (Sanger & Barnes, 2020).

حملات سایبری ذکر شده فوق تنها بخشی از صدها حملاتی بوده است که در یک دهه گذشته توسط دشمنان جمهوری اسلامی ایران بر علیه تاسیسات و زیرساخت‌های حیاتی این کشور طراحی، مهندسی و اجرا گردید است و درصد بالایی از این حملات نیز بخشی از عملیات پروژه نیترو زئوس و یا پروژه بازی‌های المپیک ایالات متحده آمریکا بر علیه ایران بوده است. از طرفی آمریکا با ترور فرمانده سپاه قدرس ایران در سال ۲۰۲۰ و با علم بر ماهیت استکبارستیزی جمهوری اسلامی ایران، این واقعیت را به خوبی درک نموده است که جمهوری اسلامی ایران هیچ‌گاه شریک سازگار با منافع استراتژیک آمریکا در منطقه نخواهد شد. بنابراین، برای مدیریت روابط خود با این کشور، باید بر اساس این واقعیت، تصمیمات اساسی مهمی در روندهای بعدی به خصوص در حوزه سایبری بر علیه این کشور اتخاذ نماید.

٤-۲- ابعاد اقدامات سایبری ایران بر علیه آمریکا

سرمایه‌گذاری‌ها و فعالیت‌های روبه گسترش ایران در فضای سایبری از ابتدای قرن بیست‌ویکم تاکنون، در کنار گفتمان هیات حاکمه این کشور درباره لزوم افزایش سرمایه‌گذاری در فضای سایبر، منجر به ارزیابی مجدد درک این کشور از قابلیت‌های خود در فضای سایبری شده است. «تجربیات گذشته ایران به خصوص در مقابله با حمله موسوم به استاکس‌نت که در سال ۲۰۱۰ سیستم‌های هسته‌ای ایران را هدف قرار داد، ضمن اینکه تأثیر زیادی در کیفیت اقدامات مقابله‌جویانه سایبری ایران در قبال آمریکا گذاشته است، در توسعه توانمندی‌های این کشور در فضای مجازی و توجه هم‌زمان به دو مفهوم حمله و دفاع نیز بسیار موثر بوده است» (Cilluffo, 2012: 3). در حالی که این حمله برنامه غنی‌سازی اورانیوم ایران را چندین سال به عقب انداخت، اما به عنوان نیروی محرکه‌ای برای ایران در جهت سرمایه‌گذاری در دفاع سایبری و قابلیت حمله سایبری ظاهر شد» (Shafa, 2014).

علاوه بر آن «اقدامات آمریکا بر علیه ایران به خصوص وضع تحریم‌های گسترده اقتصادی باعث شده جمهوری اسلامی ایران نیز در برابر فشارهای مختلف به ویژه اقتصادی علیه خود، نوعی مکانیزم دفاعی نظیر قدرت سایبری ایجاد کند. دولت ایران برای اینکه بتواند یک بازیگر قوی در حوزه سایبری شود، تلاش کرده است تا زیرساختی مستحکم هم از نظر فیزیکی و هم از نظر شیوه بازیگری ایجاد کند. این کشور برای ارتقای این مهارت‌ها، حملات سایبری را علیه مؤسسات و سازمان‌های ایالات متحده و هم‌پیمانان این کشور انجام داده است. اعتقاد بر این است که در نتیجه توسعه فناوری‌های سایبری و کیفیت حملات ایران ، این کشور در حال تبدیل شدن به یکی از قدرت‌های سایبری پیشرو در جهان است و بازیگری است که می‌تواند به زیرساخت‌های فیزیکی مورد حمله آسیب جدی وارد کند. اعتباری که دولت ایران در این حوزه به دست آورده است را در تحقق محاسبات استراتژیک خود در حوزه‌های دیگر و به راه انداختن یک جنگ نامتقارن علیه کشورهایی که با آنها در تقابل است به کار گرفته است. استراتژی دفاعی و هجومی ایران در فضای سایبری ناشی از نیاز به ایجاد تاب‌آوری اقتصادی و فناوری و عزم ایران برای خنثی کردن تهدیدات داخلی و خارجی است»(Bulut, 2021: 185). اما در این میان، سوالی که به ذهن خطور می‌کند این است که آیا توانایی حمله سایبری پیچیده ایران به سطحی رسیده است که دولت ایالات متحده را ملزم به نگرانی در مورد پیامدهای آن کند؟

دولت ایران اعلام کرده است که از آغاز قرن بیست‌ویکم، بخش قابل توجهی از بودجه این کشور به توسعه قابلیت‌های سایبری اختصاص یافته است. ادعا می‌شود که بودجه امنیتی مذکور به ویژه در دوره ریاست جمهوری حسن روحانی که در سال ۲۰۱۳ روی کار آمد، دوازده برابر شده است (Schaefer, 2018). سردار سرتیپ غلامرضا جلالی رئیس سازمان پدافند غیر عامل ایران در هشتمین مجمع ملی پدافند غیر عامل که آبان ماه ۱۳۹۸ در تهران برگزار شد، از اتخاذ رویکرد دفاعی جدید در قبال تهدیدات ترکیبی و چندلایه و تولید محصولات دفاعی برای استفاده در فضای مجازی خبر داد. (Fars News Agency, 2019). به این ترتیب، «ایران قصد دارد یک سیستم دفاعی چند بُعدی ایجاد کند که شامل فعالیت‌های نظارتی و بازرسی علیه بازیگرانی است که علیه این کشور در فضای سایبری عمل می‌کنند. برای این منظور، ایران با دو هدف اصلی پیش می‌رود: ۱. مقابله با اقدامات مخرب سایبری علیه زیرساخت‌های حیاتی و برنامه غنی‌سازی اورانیوم؛ ۲. مقابله با جاسوسی سایبری. اگرچه بیانیه ایران تا حدودی هدف این کشور در فضای سایبر را مشخص می‌کند، اما کشف توانمندی‌های این کشور در حوزه سایبری به دلیل محدودیت منابع اطلاعاتی و عدم دسترسی به استاد محرمانه بسیار مشکل می‌باشد»(Siboni & Kronenfeld, 2014: 84-85).

در مارس ۲۰۱۲، رهبر جمهوری اسلامی ایران، تشکیل شورای عالی فضای سایبری را اعلام کرد. هدف اصلی این شورا، توسعه روش‌های جدید به منظور کنترل سیستم‌های دفاعی شبکه‌های

رایانه‌ای ایران و نفوذ به شبکه‌های رایانه‌ای که تهدید محسوب می‌شوند و در مواقع ضروری نیز حمله به آن‌ها است (Harris, 2014). «این شورا که مدیریت هر دو قابلیت سایبری تهاجمی و تدافعی را بر عهده دارد، با نهادهای مختلف اطلاعاتی و امنیتی جمهوری اسلامی ایران همکاری می‌کند» (Congressional Research Service, 2020: 1).

امروزه ایران از طریق طیفی از بازیگران، از هکرهایی که با انگیزه‌های میهن‌پرستی یا مالی فعالیت می‌کنند، تا پیمانکاران بخش خصوصی، درگیر فعالیت‌های سایبری است. ادعا می‌شود که جامعه هکرهای ایرانی یکی از مسلط‌ترین و فعال‌ترین گروه‌های فعال در عرصه جهانی فضای سایبر می‌باشند. طبق نتایج حاصل از تحقیقات سایت هکری Zone-H که به تحلیل فعالیت‌های هکرها در فضای سایبری می‌پردازد، آمده است که از ۴۰ گروه فعال هکری در جهان، ۷ مورد مربوط به ایران است (Siboni & Kronenfeld, 2014: 84-85). با این حال، «فعالیت‌های انجام شده توسط ایران در حوزه سایبری در سال‌های اخیر، باعث تغییر و ارزیابی مجدد تلقی از قدرت این کشور در حوزه سایبری شده است. در این زمینه، تلاش‌هایی از سوی بازیگران مختلف برای تعریف قابلیت‌های احتمالی سایبری ایران در حال انجام است. به عنوان مثال، طبق گزارشی که مایکروسافت در مارس ۲۰۱۹ منتشر کرد، عنوان شد که گروه‌های سایبری مرتبط با ایران با حمله به هزاران نفر و بیش از ۲۰۰ شرکت در سراسر جهان در دو سال گذشته، آسیب‌های اقتصادی قابل توجهی را وارد کرده‌اند» (McMillan, 2019). «به گفته برخی از مفسران، امضا توافقنامه برجام در سال ۲۰۱۵، فرصت‌هایی را برای ایران فراهم نمود تا از طریق گسترش همکاری‌ها با دانشگاه‌ها و مؤسسات علمی در سراسر جهان، قابلیت‌های سایبری خود را توسعه دهد»(Gundert et al, 2018).

استراتژیست‌های ایالات متحده تخمین می‌زنند که مزیت نظامی نسبی و ظرفیت فعلی ایالات متحده برای انجام عملیات علیه یک دشمن پیچیده، کاهش یافته است. دشمنان بالقوه، نظیر ایران، اقدامات متعددی برای منحرف کردن کارایی قدرت نظامی ایالات متحده انجام داده‌اند که وضعیت نامطلوبی را برای این کشور ایجاد نموده است. رشد توانایی‌های هوایی، زمینی و دریایی دشمنان بالقوه با قابلیت‌های حمله توسعه‌یافته در فضای سایبری، آنها را قادر می‌سازد تا با نیروهای آمریکایی در مناطقی که سلطه ایالات متحده از مدت‌ها پیش فرض شده است، مبارزه کنند (Tikk, 2019:25). از این‌رو، «این کشور در یک دهه گذشته، با هجوم عملیات‌های سایبری تهاجمی متعددی از سوی ایران و نیروهای نیابتی این کشور مواجه بوده است که بخش‌های زیرساختی حیاتی و شرکت‌های تجاری ایالات متحده و هم‌پیمانان این کشور را مورد هدف قرار داده است. آژانس امنیت سایبری و امنیت زیرساخت ایالات متحده آمریکا[1] شانزده بخش را که هدف تهدیدات سایبری فعال بوده‌اند

[1]. Cybersecurity and Infrastructure Security Agency (CISA)

را شناسایی کرد. از میان شانزده بخش، انرژی، مراقبت‌های بهداشتی و پایگاه‌های صنعت دفاعی[1] همچنان شاهد افزایش حملات از سوی جمهوری اسلامی ایران می‌باشند»(Fischerkeller, 2017).

جمهوری اسلامی ایران در طول یک دهه گذشته، همواره یکی از متهمان اصلی حملات سایبری به زیرساخت‌های حیاتی آمریکا بوده است. «حملات سایبری ایران علیه آمریکا به سال ۲۰۰۹ میلادی و هنگامی باز می‌گردد که گروه ارتش سایبری ایران در پاسخ به اعتراضات جنبش سبز، به دلیل انتخاب مجدد رئیس‌جمهور محمود احمدی‌نژاد در ایران، صفحه اصلی توییتر را هک کرد»(Kaminski, 2020: 64-70). «حملات سایبری از منظر ایران، بخشی از توانایی نظامی نامتقارن و دفاعی در مقابل آمریکاست و توسعه قدرت سایبری ایران نیز واکنشی به آسیب‌پذیری‌های گذشته و قرار داشتن به عنوان یک هدف حملات سایبری بوده است»(Lewis, 2019).

بلافاصله پس از اعلام تصمیم رئیس جمهور آمریکا، ترامپ، مبنی بر خروج از برجام در ماه می ۲۰۱۸، حملات سایبری منتسب به ایران بر علیه آمریکا و متحدان آن بالافاصله آغاز شد. سرعت شکل‌گیری این حملات به حدی بود که بسیاری از کارشناسان بر این باورند که آمادگی برای یک حمله سایبری در پاسخ به خروج احتمالی آمریکا از برجام، از قبل توسط ایران طراحی و برنامه‌ریزی شده بود. در ژوئن ۲۰۱۹ نیز اعلام شد که عملیات سایبری تهاجمی ایران علیه آمریکا، پس از اعمال تحریم‌های جدید دولت ترامپ علیه بخش پتروشیمی ایران تشدید شد (Bulut, 2021: 183).

در اولین روزهای سال ۲۰۲۰، با ترور سردار قاسم سلیمانی فرمانده نیروی قدس سپاه پاسداران ایران که عملیات برون مرزی این کشور را رهبری می‌کرد، به دست ارتش ایالات متحده آمریکا، فضای سایبری در کنار فضای فیزیکی خود را برای ورود به یک فرایند جدیدی از تقابل میان آمریکا و ایران آماده نمود. پس از این ترور، ارزیابی‌های گسترده آمریکا حاکی از آن بود که پاسخ ایران به آمریکا محدود به دنیای فیزیکی نخواهد بود. و لذا هشدارهای مختلفی از سوی مقامات آمریکایی داده شد که ایران با استفاده مشترک از تکنیک‌های جنگ فیزیکی و سایبری علیه آمریکا و متحدانش، این اقدام آمریکا را در سطوحی گسترده تلافی خواهد کرد.

٤-٣- آینده‌نگری تاثیرات فناوری‌های سایبری در روابط میان ایران و آمریکا

توسعه فزاینده وابستگی کشورها به زیرساخت‌های دیجیتال، آسیب‌پذیری‌های استراتژیک آنها را افزایش خواهد داد. اکثر کشورها منابع قابل توجهی مبتنی بر فناوری اطلاعات و ارتباطات از جمله سیستم‌های دفاعی، سیستم‌های مدیریت عمومی، سیستم‌های مدیریت پیچیده و زیرساخت‌های اطلاعاتی دارند که شامل کنترل برق، سیستم تلفن، جریان پول، ترافیک هوایی، جریان نفت و گاز، فناوری‌های هوشمند نظیر رباط‌های هوشمند جراحی از راه دور، خانه‌های هوشمند، وسایل نقلیه هوایی و زمینی خودران و غیره می‌شود. جامعه روز به روز به فناوری اطلاعات و ارتباطات بیشتر

[1]. Defense industrial base (DIB)

وابسته می‌شود. که این امر هم به دلیل افزایش تعداد کاربران و هم به دلیل روند اتصال شبکه‌های کامپیوتری به یکدیگر، حساسیت بیشتری را در پی خواهد داشت. در این راستا، حفاظت از زیرساخت‌های اطلاعاتی به عنوان یکی از اولویت‌های امنیت ملی تحمیل می‌شود. در نتیجه‌ی نیازهای اجتماعی و نوآوری‌های تکنولوژیکی‌های آتی، فضای مجازی نیز به فضای تعاملی نامحسوس و نامحدودتری تبدیل خواهد شد که توسط شبکه‌های کامپیوتری ایجاد شده‌اند. با گذشت زمان و توسعه فناوری‌های نوین سایبری، عملیات‌های سایبری تهاجمی برای پشتیبانی از عملیات نظامی نیز رو به گسترش خواهد بود. هنگام برنامه‌ریزی ماموریت‌های آشکار یا پنهان، باید به تأثیر اقدامات فضای سایبری بر نتیجه مأموریت‌های پیش‌رو توجه نمود.

سطح تهدیدات عملیات‌های سایبری در آینده به مراتب خطرناک‌تر و گسترده‌تر خواهد بود. از این‌رو، توانمندی‌ها و اقدامات سایبری میان ایالات متحده آمریکا و جمهوری اسلامی ایران که در سرتاسر این پژوهش به آنها اشاره شده است به این واقعیت اشاره می‌کند که حملات سایبری بعدی در مقیاسی بسیار بزرگ‌تر در آینده در کمین این دو کشور خواهد بود. با ادامه افزایش تنش‌ها میان این دو کشور در محیط فیزیکی، اقدامات سایبری آن دو نیز در قبال یکدیگر، احتمالا نقشی اساسی در نتایج هرگونه درگیری احتمالی در آینده ایفا خواهد کرد.

٤-٤- راه‌کار پیشنهادی در تقابل سایبری با آمریکا

محرمانه بودن اقداماتی که یک دولت برای اطمینان از امنیت سایبری زیرساخت‌های حیاتی خود ایجاد می‌کند، می‌تواند به عنوان اصل اساسی پذیرفته شود. با این حال، زمانی که ویژگی جهانی‌بودن فضای سایبری مد نظر باشد، نیاز به اتحاد و همکاری بین‌المللی امنیت سایبری بر اساس اصل وابستگی متقابل وجود دارد. بنابراین، امنیت سایبری زیرساخت‌های مشترک و حیاتی، نه‌تنها یک موضوع ملی است، بلکه نیازمند همکاری بین‌المللی نیز می‌باشد. بیشتر تهدیدات فضای مجازی، از بیش از یک متغیر تشکیل شده است. چند بُعدی بودن نسل جدید تهدیدات ناشی از تحولات فناوری، رویکردهای جدید و گسترده‌ای را در راهبردهای امنیت ملی کشورها الزامی می‌کند. تامین امنیت سایبری بخش‌های زیرساختی حیاتی که اکنون به عنوان اهداف نظامی دیده می‌شوند، برای بقای دولت‌ها ضروری است. به خصوص در ۲۰ سال گذشته، زیرساخت‌های حیاتی به شدت به فرآیندهای وابسته به فناوری‌های شبکه متکی بوده است. این شرایط تامین امنیت سایبری برای زیرساخت‌های حیاتی را به یک هدف بسیار مهم از استراتژی‌های امنیت ملی دولت‌ها تبدیل کرده است. از این‌رو، توسعه دفاع سایبری و تقویت ظرفیت حمله، در تعیین استراتژی‌های دفاع ملی کشورها امروزه بیش از هر زمان دیگری ضروری است (Burak & Soner, 2022: 273).

برای جمهوری اسلامی ایران ضروری است که یک استراتژی امنیتی یکپارچه برای حفاظت از زیرساخت‌های حیاتی وابسته به شبکه و تعیین اقدامات امنیت سایبری و امنیت فیزیکی ایجاد کنند.

این کشور باید یک رویکرد جامع و یکپارچه اتخاذ کند که در آن خطرات و تهدیدها در عرصه فضای سایبر از همه زوایا ارزیابی شده و نقش همه بازیگران مربوطه برای دوره‌های قبل، حین و پس از حمله سایبری تعریف شود. با تفکر یک هکر یا تروریست، باید ضعیف‌ترین و حساس‌ترین نقاط زیرساخت‌های حیاتی خود را شناسایی کرد، بدترین سناریوها را پیش‌بینی و برای آن آماده شد و اقدامات لازم برای پیشگیری و پاسخ به این سناریوها را نیز مشخص کرد. پس از ایجاد ساختاری که بتواند همه این عناصر را سازماندهی کند، یک سیستم مدل، مورد نیاز است. باید تصمیم گرفته شود که در صورت حمله سایبری، چه کسی، چه زمانی و به چه شکلی واکنش نشان دهد. بررسی و پرداختن به جزئیات این مسائل از اهمیت بالایی برخوردار است. اولویت‌ها در این زمینه شامل تعیین گام‌های لازم برای پیشگیری، حفاظت و بازیابی است.

فعالیت‌های فضای سایبری که ایران با حمایت بازیگران نیابتی خود در خارج از کشور به نمایش گذاشته است را می‌توان بخشی از استراتژی این کشور در برابر تحولات ژئوپلیتیکی دانست. این کشور در راستای مقابله با سیاست‌های ضد ایرانی ایالات متحده آمریکا، می‌تواند از روش‌هایی استفاده نماید که آسیب کمتری به وجهه این کشور در سطوح بین‌الملل وارد نماید. بنابراین، این انتظار درست‌تر است که از ایران انتظار داشته باشیم که به جای اینکه سیاست‌های خود را در قبال آمریکا به حداقل برساند، در فعالیت‌هایی که بیشتر به وجهه آن لطمه نمی‌زند و در طول زمان و از طریق نمایندگان خود در منطقه گسترش می‌یابد، اقدام نماید.

نتیجه‌گیری

با رشد فناوری‌های ارتباطی شبکه محور، تامین امنیت زیرساخت‌های حیاتی توسط یک دولت در تضمین امنیت ملی، از اهمیت حیاتی برخوردار شد. بستر ارتباطی اینترنت و فضای سایبر، دارای پتانسیل ایجاد الگوهای نوین کنش‌گری میان دولت‌ها، انسان‌ها و حتی بازیگران غیر دولتی نظیر سازمان‌ها، شرکت‌ها، تروریست‌ها و غیره می‌باشد. با رشد فناوری‌های ارتباطی شبکه محور، تامین امنیت زیرساخت‌های حیاتی توسط یک دولت در تضمین امنیت ملی، از اهمیت حیاتی برخوردار شد. زیرا امروزه کشورها شروع به پذیرش زیرساخت‌های حیاتی یکدیگر به عنوان یک هدف نظامی کرده‌اند. از این رو حصول اطمینان از امنیت سایبری زیرساخت‌های حیاتی، همچنان اهمیت خود را از نظر امنیت دولتی افزایش می‌دهد، زیرا پیشرفت‌های فناوری شبکه‌محور، همچنان در حال تکامل می‌باشند.

جمهوری اسلامی ایران و آمریکا از جمله کشورهایی می‌باشند که روابط میان آن دو، از سال ۲۰۰۹ تا کنون و در پی حملات سایبری به تاسیسات هسته‌ای ایران از سوی آمریکا، متاثر از فضای تعاملی سیاست و سایبر در عرصه‌های نظری و عملی بوده است. پژوهش حاضر به دنبال پاسخ‌گویی به این پرسش بوده است که شیوه‌های نوین تقابل میان ایران و آمریکا در فضای سایبر چه می‌باشد؟

در راستای پاسخ به سوال پژوهش، با استفاده از روش توصیفی-تحلیلی جهت آزمون فرضیه و روش کتابخانه‌ای و فیش‌برداری برای گردآوری داده‌ها و اطلاعات، در کنار بکارگیری مولفه‌ها و گزاره-های نظریه قدرت اجبار، این نتایج حاصل گردیده است که ایالات متحده آمریکا و جمهوری اسلامی ایران، هر یک با توجه به سطح توانمندی و مقدورات خود در حوزه فناوری‌های نوین سایبری، به نحوی از این توانمندی به عنوان ابزار اعمال قدرت و اجبار بر علیه طرف مقابل جهت اعمال زور و تحمیل اراده بهره‌برداری نموده‌اند.

در همین راستا، آمریکا با استفاده از قابلیت‌ها و توانمندی‌های خود در حوزه فناوری‌های نوین سایبری و بهره‌گیری از جدیدترین و مدرن‌ترین ابزارهای مخرب این حوزه، نظیر بدافزارهایی چون استاکس نت، فلیم، دوکو و غیره، به کرات زیرساخت‌های حیاتی تحت شبکهِ جمهوری اسلامی ایران را آماج حملات مخرب سایبری خود قرار داد و خسارات گسترده‌ای را بهِ جمهوری اسلامی ایران تحمیل نموده است، تا از این طریق بتواند این کشور را به تغییر رفتار و مواضع و یا پذیرش خواسته‌های خود مجبور نماید.

در مقابل، استراتژی پیگیری شده توسط دولت ایران در حوزه سایبری در دو دهه اخیر را می‌توان به عنوان پاسخ‌های تلافی‌جویانه و توسعه‌یافته علیه تنش‌های ژئوپلیتیک در سطوح منطقه‌ای یا بین-المللی برخواسته از اقدامات ایالات متحده آمریکا و هم‌پیمانان این کشور ارزیابی کرد. در این زمینه، مشاهده می‌شود که ایران مکانیسمی باثبات برای استفاده از فعالیت‌های تهاجمی در فضای سایبری، برای پاسخ‌گویی به رویدادهای ژئوپلیتیک ارائه کرده است. این روند به این معناست که استراتژی سایبری ایران در قبال آمریکا با منافع ژئوپلیتیکی این کشور مرتبط است، به طوری که استراتژی سایبری خود را بر اساس روند شکل‌دهی این منافع طراحی نموده است. در شرایط کنونی، اگرچه ایران به عنوان یکی از قدرت‌های پیشروِ سایبری جهان به حساب نمی‌آید، اما به‌عنوان بازیگری مطرح می‌شود که ضمن گسترش فعالیت‌هایِ خود در فضای سایبر، توانسته است از نظر تراکم، تنوع و تخریب سایبری، جایگاه خود را به روند رو به رشدی تقویت نماید.

منابع فارسی

۱. صانعیان، ع. (۱۳۹۸). امنیت سایبری در آمریکا؛ ساختارها و روندها. *فصلنامه سیاست خارجی*، ۳۳(۱)، ۱۹۱-۲۲۸.

۲. علیخانی، م. (۱۳۹۹). بررسی راهبرد فشار حداکثری ترامپ بر ایران از منظر «قدرت اجبار». *فصلنامه مطالعات بین‌المللی*، ۱۷(۱)۶۵، ۸۶-۶۳ .

۳. لرستانی، ع. (۱۳۹۷). مروری بر روش‌های مقابله با بدافزارها و نرم‌افزارهای جاسوسی. *فصلنامه مطالعات حفاظت و امنیت انتظامی*، ۱۳(۴۹)، ۱۵۲-۱۲۵.

۴. موحدیان، ا. (۱۳۹۹). *سایبر دیپلماسی آمریکا در قبال ایران در دوره ریاست جمهوری باراک اوباما*، تهران: نشر ایرانا رسانه.

English References

1. Baezner, M. (2019). Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions. Zurich: *Center for Security Studies*, at: https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions.
2. Barnes, J., Gibbons, T. (2019). U.S. Carried Out Cyberattacks on Iran. *The New York Times*. at: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
3. Bulut, S. (2021). Iran's Cyberspace Activities: Findings on the Joint Comprehensive Plan of Action Process. *Gaziantep University Journal of Social Sciences*, Vol. 20(1), 166-19, at: file:///C:/Users/ASUS/Desktop/10.21547-jss.718313-1047027.pdf
4. Burak, A., Soner, C. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. *Perception: Journal of International Affairs*, Vol. 26(2), 259–276, at: https://dergipark.org.tr/en/pub/perception/issue/68005/1055264.
5. Cilluffo, Frank J. (2012). The Iranian Cyber Threat to the United States, *The George Washington University*, Homeland Security Policy Institute, at: https://www.govinfo.gov/content/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm.
6. Congressional Research Service. (2020, January 13). Iranian Offensive Cyber Attack Capabilities. at: https://sgp.fas.org/crs/mideast/IF11406.pdf.
7. Craig, A., Valeriano, B. (2016). *Conceptualising cyber arms races. 8th International Conference on Cyber Conflict (CyCon)*. Tallinn: NATO CCD COE Publications, pp. 141-158
8. Eisenstadt, M. (2016). Iran's Lengthening Cyber Shadow. *The Washington Institute for Near East Policy*, 34, 1-19.
9. Epps, D. (2021). *Offensive Cyber Operations Reshaping the Modern Battlespace*. New York, Utica College, M.A. Thesis, of Cybersecurity at: https://www.proquest.com/openview/175887c1b151855dd298a55aaf3b536f/1?pq-origsite=gscholar&cbl=18750&diss=y.
10. Fars News Agency. (2019). Iran Opts for New Civil Defense Approach to Confront US Threats. at: http://fna.ir/dd595c.

11. Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional. *Deterrence Strategies. Survival*, Vol. 59(1), 103–134. at: https://doi.org/10.1080/00396338.2017.1282679.
12. Fixler, A. (2020). The Cyber Threat from Iran after the Death of Soleimani. *CTC Sentilel*, Vol. 13(2), 1-40.
13. Goel, S. (2020). How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections The Quarterly Journal*, Vol. 19(1), 87-95
14. Gompert, D. C., Binnendijk, H. (2016). The Power to Coerce, Countering Adversaries Without Going to War. at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1000/RAND_RR1000.pdf.
15. Gundert, L., Chohan, S., Lesnewich, G. (2018). Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations. at: https://www.recordedfuture.com/iran-hacker-hierarchy/.
16. Harris, S. (2014). Forget China: Iran's Hackers Are America's Newest Cyber Threat," Foreign Policy. at: https://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/.
17. Kaminski, M. (2020). *Operation "Olympic Games." Cyber-sabotage as a tool of American Intelligence aimed at counteracting the development of Iran's Nuclear Program. Security Defence, Faculty of National Security*. War Studies University, Warsaw, Poland, at: http://doi.org/10.35467/sdq/121974.
18. Katzman, K. (2020). U.S.-Iran Conflict and Implications for U.S. Policy. Congressional Research Service, Updated May 8, 2020, at: https://fas.org/sgp/crs/mideast/R45795.pdf.
19. Kronenfeld, S., Siboni, G. (2014). Developments in Iranian Cyber Warfare. M*ilitary and Strategic Affairs*, Vol. 6(2), 83-104.
20. Lewis, J. A. (2019). Iran and Cyber Power. Center for Strategic and International Studies: CSIS, June 25, at: https://www.csis.org/analysis/iran-and-cyber-power?amp.
21. McMillan, R. (2019). Iranian Hackers Have Hit Hundreds of Companies in Past Two Years. *Wall Street Journal*, at: https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

22. Sanger, D., Barnes, J. (2020). U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came. *The New York Times*, at: https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.
23. Schaefer, B. (2018). The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism. Georgetown Security Studies Review, at: https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism.
24. Shafa, E. (2014). Iran's Emergence as a Cyber Power. United States Army War College, at: https://vdocuments.net/reader/full/irans-emergence-as-a-cyber-power.
25. Tikk, E. (2019). *Cyber arms control and resilience*. Yearbook- Armaments, Disarmament and International Security, Oxford University Press.
26. Utinková, H. (2021). *Cyber-attacks Against Iran as Instruments of Hybrid Warfare*. Master's Thesis. Charles University, Institute of Political Studies, Department of Security Studies.
27. Vuletic, D., Milenkovic, M., Dukic, A. (2021). Cyberspace as a domain of conflict: The case of the United States - Iran and North Korea. *Military work Journal*, University of Defence, Strategic Research Institute, Belgrade, Vol. 73(1), 1-14
28. Zetter, K. (2012). Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. at: https://www.wired.com/2012/05/flame.

Translated References to English

1. Alikhani, M. (2020). Examining Trump's "Maximum Pressure Strategy" on Iran from the Perspective of "Coercive Power". *International Studies Journal* (ISJ), 17(1), 63-86. doi: 10.22034/isj.2020.119268 **(In Persian)**
2. Baezner, M. (2019). Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions. Zurich: *Center for Security Studies*, at: https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions.
3. Barnes, J., Gibbons, T. (2019). U.S. Carried Out Cyberattacks on Iran. *The New York Times*. at: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
4. Bulut, S. (2021). Iran's Cyberspace Activities: Findings on the Joint Comprehensive Plan of Action Process. *Gaziantep University Journal of Social Sciences*, Vol. 20(1), 166-19,

at: file:///C:/Users/ASUS/Desktop/10.21547-jss.718313-1047027.pdf

5. Burak, A., Soner, C. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. *Perception: Journal of International Affairs*, Vol. 26(2), 259–276, at: https://dergipark.org.tr/en/pub/perception/issue/68005/1055264.
6. Cilluffo, Frank J. (2012). The Iranian Cyber Threat to the United States, *The George Washington University*, Homeland Security Policy Institute, at: https://www.govinfo.gov/content/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm.
7. Congressional Research Service. (2020, January 13). Iranian Offensive Cyber Attack Capabilities. at: https://sgp.fas.org/crs/mideast/IF11406.pdf.
8. Craig, A., Valeriano, B. (2016). *Conceptualising cyber arms races. 8th International Conference on Cyber Conflict (CyCon)*. Tallinn: NATO CCD COE Publications, pp. 141-158
9. Eisenstadt, M. (2016). Iran's Lengthening Cyber Shadow. *The Washington Institute for Near East Policy*, 34, 1-19.
10. Epps, D. (2021). *Offensive Cyber Operations Reshaping the Modern Battlespace*. New York, Utica College, M.A. Thesis, of Cybersecurity at: https://www.proquest.com/openview/175887c1b151855dd298a55aaf3b536f/1?pq-origsite=gscholar&cbl=18750&diss=y.
11. Fars News Agency. (2019). Iran Opts for New Civil Defense Approach to Confront US Threats. at: http://fna.ir/dd595c.
12. Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional. *Deterrence Strategies. Survival*, Vol. 59(1), 103–134. at: https://doi.org/10.1080/00396338.2017.1282679.
13. Fixler, A. (2020). The Cyber Threat from Iran after the Death of Soleimani. *CTC Sentilel*, Vol. 13(2), 1-40.
14. Goel, S. (2020). How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections The Quarterly Journal*, Vol. 19(1), 87-95
15. Gompert, D. C., Binnendijk, H. (2016). The Power to Coerce, Countering Adversaries Without Going to War. at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1000/RAND_RR1000.pdf.

16. Gundert, L., Chohan, S., Lesnewich, G. (2018). *Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations*. at: https://www.recordedfuture.com/iran-hacker-hierarchy/.
17. Harris, S. (2014). Forget China: Iran's Hackers Are America's Newest Cyber Threat," Foreign Policy. at: https://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/.
18. Kaminski, M. (2020). *Operation "Olympic Games." Cyber-sabotage as a tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Program. Security Defence, Faculty of National Security*. War Studies University, Warsaw, Poland, at: http://doi.org/10.35467/sdq/121974.
19. Katzman, K. (2020). U.S.-Iran Conflict and Implications for U.S. Policy. Congressional Research Service, Updated May 8, 2020, at: https://fas.org/sgp/crs/mideast/R45795.pdf.
20. Kronenfeld, S., Siboni, G. (2014). Developments in Iranian Cyber Warfare. M*ilitary and Strategic Affairs*, Vol. 6(2), 83-104.
21. Lewis, J. A. (2019). Iran and Cyber Power. Center for Strategic and International Studies: CSIS, June 25, at: https://www.csis.org/analysis/iran-and-cyber-power?amp.
22. Lorestani, A. (2019). A review of methods to deal with malware and spyware. *Disciplinary Security and Protection Studies Journal*, 13(49), 125-152. **(In Persian)**
23. McMillan, R. (2019). Iranian Hackers Have Hit Hundreds of Companies in Past Two Years. *Wall Street Journal*, at: https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.
24. Movahedian, E. (2020). US *Cyber Diplomacy Towards Iran During Barack Obama's Presidency*. Tehran: Irana Media. **(In Persian)**.
25. Saneian, A. (2019). Cyber Security in America; Structures and trends. *Foreign Policy Journal*, 33(1),191-228. **(In Persian)**.
26. Sanger, D., Barnes, J. (2020). U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came. *The New York Times*, at: https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.
27. Schaefer, B. (2018). The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism. Georgetown Security Studies Review, at: https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism.

29. Shafa, E. (2014). Iran's Emergence as a Cyber Power. United States Army War College, at: https://vdocuments.net/reader/full/irans-emergence-as-a-cyber-power.
30. Tikk, E. (2019). *Cyber arms control and resilience*. Yearbook- Armaments, Disarmament and International Security, Oxford University Press.
31. Utinková, H. (2021). *Cyber-attacks Against Iran as Instruments of Hybrid Warfare*. Master's Thesis. Charles University, Institute of Political Studies, Department of Security Studies.
32. Vuletic, D., Milenkovic, M., Dukic, A. (2021). Cyberspace as a domain of conflict: The case of the United States - Iran and North Korea. *Military work Journal*, University of Defence, Strategic Research Institute, Belgrade, Vol. 73(1), 1-14
33. Zetter, K. (2012). Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. at: https://www.wired.com/2012/05/flame.