Journal iranian political sociology

Vol. 4, No.4, winter2022

https://dx.doi.org/10.30510/psi.2022.315683.2651

New State-Nation Security Challenges in Cyberspace with Emphasis on the Islamic Republic of Iran

Abstract

In the last two decades, security challenges in cyberspace have been the ultimate current problem of governments with cyberspace and network-based infrastructure. The entanglement of today's world in the age of communication and information technology, in addition to the unique opportunities it has created for nation-states, has also raised concerns. One of these concerns is the national security issues of nation-states, which have been severely threatened by organized and destructive cyber activities. This research uses a descriptive-analytical method to test the hypothesis and a library and phishing method to collect data and information, along with the use of Castells's network community theory, to answer this question. The question is what are the new security challenges of the nation-state in cyberspace with emphasis on the Islamic Republic of Iran? The results of this study indicate that new cyber technologies, despite opening up irreplaceable opportunities in the military, economic, cultural, political and social spheres for the advancement of nation-states, But at the same time, it has jeopardized national security and interests. In the meantime, the Islamic Republic of Iran, due to the fact that most of its economic, commercial, cultural, social and governmental activities and interactions are carried out at all levels, including individuals, non-governmental organizations and governmental and governmental institutions in cyberspace. Hence, over the past decade, it has always been under widespread cyber-attack by its enemies, and therefore has suffered great damage at various material and spiritual levels. This has led the country to place a high profile on the issue of cyber deterrence in its defense strategy.

Keywords: Islamic Republic of Iran, cyberspace, new security challenges, national security

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره چهارم(پیاپی۱٦)زمستان۱٤۰۰،صص۳۵۰-۳۲٦

https://dx.doi.org/10.30510/psi.2022.315683.2651

چالش‌های نوین امنیتی دولت-ملت در فضای سایبر با تاکید بر جمهوری اسلامی ایران

رضا سلگی[۱]

حسن خداوردی[۲]

زهره پوستین‌چی[۳]

تاریخ دریافت : ۱٤۰۰/۰۷/۲۷

تاریخ پذیرش: ۱٤۰۰/۰۹/۱۸

چکیده

در دو دهه گذشته چالش‌های امنیتی در فضای سایبر، حد نهایت معضلات کنونی دولت‌های برخوردار از زیرساخت‌های متکی به فضای سایبر و شبکه بوده است. درهم تنیدگی دنیای کنونی در عصر ارتباطات و فناوری اطلاعات، در کنار فرصت-های بی‌نظیری که برای دولت-ملت‌ها به‌وجود آورده است، نگرانی‌هایی را نیز در پی داشته است. یکی از این نگرانی‌ها، مسائل مربوط به امنیت ملی دولت-ملت‌هاست که فعالیت‌های سازمان‌یافته و مخرب سایبری، آن را به‌شدت تهدید نموده است. این پژوهش با استفاده از روش تفسیری- کیفی جهت آزمون فرضیه و روش کتابخانه‌ای و فیش‌برداری برای گردآوری داده‌ها و اطلاعات، درکنار بهره‌گیری از نظریه جامعه شبکه‌ای کاستلز، به دنبال پاسخ‌گویی به این پرسش می‌باشد که چالش‌های نوین امنیتی دولت-ملت در فضای سایبر با تاکید بر جمهوری اسلامی ایران چه می‌باشد؟ نتایج حاصل از این پژوهش گویای این مطلب است که تکنولوژی‌های نوین سایبری، علیرغم اینکه فرصت‌های بی‌بدیلی را در حوزه‌های نظامی، اقتصادی، فرهنگی، سیاسی و اجتماعی، پیش‌روی دولت-ملت‌ها گشوده است، اما به موازات آن، امنیت و منافع ملی را به مخاطره انداخته است. در این میان، جمهوری اسلامی ایران به واسطه اینکه بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی خود را در کلیه سطوح اعم از افراد، موسسات غیردولتی و نهادهای دولتی و حاکمیتی در فضای سایبر انجام می-دهد از این‌رو، در طول یک دهه گذشته همواره مورد تهاجم گسترده سایبری از سوی دشمنان خود بوده و لذا خسارات زیادی را نیز در سطوح مختلف مادی و معنوی متحمل شده است. این امر باعث گردید تا این کشور در راهبرد دفاعی خود جایگاه والایی برای موضوع بازدارندگی در حوزه سایبر قائل شود.

واژگان کلیدی: جمهوری اسلامی ایران، فضای سایبر، چالش‌های نوین امنیتی، امنیت ملی

۱. گروه علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

۲. گروه علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران*(نویسنده مسئول: h_khodaverdi@azad.ac.ir)

۳. گروه علوم سیاسی و روابط بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

مقدمه

تکنولوژی اینترنت یکی از بزرگترین فناوری‌هایی است که تاکنون به دست انسان طراحی، مهندسی و اجرا شده است. امروزه حیات بشری مرحله نوینی از تحولات خود را با عبور از عصر اطلاعات و ارتباطات تجربه می‌کند. حاکمیت عناصر نرم‌افزاری قدرت و پیشرفت جوامع، بیشتر از هر زمان دیگری مورد توجه است. فضای سایبر عرصه جدیدی برای سیاست نیز مهیا نموده است. فضایی که در آن افراد، گروه‌های مختلف و دولت‌ها درحال بازیگری و سیاست‌ورزی هستند. اما درهم تنیدگی دنیای کنونی در عصر ارتباطات و فناوری اطلاعات، در کنار فرصت‌های بی‌نظیری که برای کشورها و جوامع مختلف به‌وجود آورده است، نگرانی‌هایی را نیز در پی داشته است. یکی از این نگرانی‌های مهم، مسائل مربوط به امنیت ملی کشورها است که فعالیت‌های مخرب سایبری، آن را به‌شدت مورد تهدید قرار می‌دهد. وابسته بودن نیازهای حیاتی بشر به فناوری‌های ارتباطی باعث گردید تا این فناوری‌ها به عنوان زیرساخت‌هایی که کار مدیریت، برنامه‌ریزی و خدمت‌دهی در زندگی روزانه مردم را بر عهده دارند، بسترهای طمع و وسوسه طرف‌های منازعه را برای تخریب اراده طرف مقابل و تحمیل اراده خود و ایجاد تفوق و سیطره فراهم آورد.

این پژوهش به دنبال پاسخ‌گویی به این سوال است که چالش‌های نوین امنیتی دولت–ملت در فضای سایبر با تاکید بر جمهوری اسلامی ایران چه می‌باشد؟ در راستای پاسخ‌گویی به سوال پژوهش این فرضیه مطرح می‌گردد که در عصر اطلاعات تقریباً تمامی امور دولت‌ها و حتی زندگی انسان‌ها به نوعی با سیستم‌های دیجیتالی و رایانه‌ای گره خورده است. به نظر می‌رسد بستر اینترنت و فضای سایبر به عنوان مولود فناوری‌های نوین اطلاعاتی و ارتباطی در طول یک دهه گذشته، به منطقه جنگی بدون حد و مرزی میان همه بازیگران و فعالان این عرصه، اعم از دولتی و غیر دولتی تبدیل شده است. از این‌رو هرگونه ایجاد اختلال و نفوذ در این سیستم‌ها می‌تواند به نوعی در به هم زدن نظم اجتماعی و امنیت ملی کشورها موثر باشد. در این میان جمهوری اسلامی ایران یکی از کشورهایی است که در طول یک دهه گذشته همواره مورد هجمه حملات متعدد سایبری مخرب از سوی دشمنان خود بوده است. و به تبع آن، امنیت ملی این کشور همواره با چالش‌های جدی روبرو بوده است. هدف از این پژوهش آن است تا با استفاده از روش تفسیری- کیفی جهت آزمون فرضیه و روش کتابخانه‌ای و فیش‌برداری برای گردآوری داده‌ها و اطلاعات، درکنار بهره‌گیری از نظریه جامعه شبکه‌ای کاستلز، به بررسی و شناخت چالش‌های نوین امنیتی دولت–ملت در فضای سایبر با تاکید بر جمهوری اسلامی ایران بپردازد.

۲- چارچوب‌نظری و ادبیات پژوهش

۲-۱- جامعه شبکه‌ای کاستلز

پرداختن به مسئله اطلاعات و ارتباطات، و تاثیری که این فناوری‌ها در عرصه‌های مختلف سیاسی، نظامی، اقتصادی و فرهنگی جوامع مختلف داشته است، امروزه به مثابه یکی از مهم‌ترین راه‌های علاج مشکلات و نماد مرکزی عصری که در آن زندگی می‌کنیم می‌باشد.

برای اولین بار در سال ۱۹۹۷ میلادی، اصطلاح «جامعه شبکه‌ای» توسط «مانوئل کاستلز» وارد ادبیات دانشگاهی شد. (عسگرخانی و دیگران،۸۲:۱۳۹۳) گسترش فزاینده فناوری اطلاعات و ارتباطات که مانوئل کاستلز از آن به عنوان جامعه شبکه‌ای یاد می‌کند، دگرگونی در حیات بشری را در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی به بار آورده و به ظهور جامعه شبکه‌ای انجامیده است. به گونه‌ای که این تحول «انقلاب صنعتی سوم» نامگذاری شده است. (Bell,2007:59)

به تعبیر کاستلز، جامعه شبکه‌ای جهانی، جامعه‌ای است که ساختارهای اجتماعی آن پیرامون شبکه‌های فعال شده از طریق فناوری‌های اطلاعاتی، ارتباطی و پردازش شده دیجیتالی و مبتنی بر میکروالکترونیک شکل گرفته است. وی مفهوم قدرت را دارای جنبه‌های مهم ارتباطی می‌داند. (کاستلز، ۱۳۹۳: ۸۳) در جامعه شبکه‌ای جهانی، همه شئون انسانی نظیر ارزش‌ها، هویت، الگوی تقسیم‌کار، مفهوم زمان و مکان و همچنین قدرت، به شبکه‌ها وابسته شده‌اند و اهداف، ویژگی‌ها، ساختار و برنامه‌های شبکه است که به تعریف شئون انسانی می‌پردازد. در این جامعه، ارزش را سلسله مراتب برنامه‌ریزی شده شبکه از طریق کنش‌گرانی که درون شبکه ایفای نقش می‌کنند، تعریف می‌کند. شبکه‌ها تسلط فضای «مکان‌ها» بر فضای «جریان‌ها» را نوید می‌دهند و شکل فضایی از جامعه ایجاد می‌شود؛ همچنین فرهنگ جامعه شبکه‌ای به فرهنگ پروتکل‌های ارتباطی تغییر می‌یابد؛ دولت-ملت دگرگون می‌شود؛ دولت شبکه‌ای ظهور می‌کند و سرانجام، قدرت در جامعه شبکه‌ای به دست کسانی می‌افتد که ظرفیت‌های ارتباطی میان شبکه‌ها و گروه‌های درون شبکه را کنترل می‌کنند. (دیوسالار،۹٤:۱۳۹۳)

۲-۲- ادبیات پژوهش

زنجانی، جواد (۱۳۹۸) در پایان‌نامه کارشناسی ارشد خود تحت عنوان «شناسایی و مقابله با تهدیدات سایبری رژیم صهیونیستی علیه ارتش جمهوری اسلامی ایران»، ضمن بررسی تهدیدات سایبری از سوی اسرائیل به این

نتیجه می‌رسد که ویژگی‌های بسیار مناسب حملات سایبری از جمله هزینه پایین و مشخص نشدن مبدا این حملات باعث گردید اسرائیل را به سمت استفاده از حملات سایبری بر علیه ایران سوق دهد. با توجه به اینکه ارتش ایران در عملیات نظامی از سامانه های هوشمند و زیرساخت ارتباطات مبتنی بر فضای سایبری بهره‌برداری می‌نماید، شناسایی شاخص‌های مقابله با تهدیدات سایبری اسرائیل می‌تواند کمک شایانی به انجام ماموریت‌های محوله و برقراری ارتباط امن و پایدار نماید.

عظیمی و خشنودی (۱۳۹۵)، در پژوهشی تحت عنوان «نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن» به این نتیجه میرسد که امروزه تروریسم از تهدیدی ملی به یک تهدید بین‌المللی تبدیل شده و خوف آن وجود دارد که با گسترش آن، صلح و امنیت بین‌المللی به مخاطره افتد. جمهوری اسلامی ایران نیز به دلیل آنکه محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی‌شماری را دربر دارد، همانند هر کشور دیگری نیازمند استراتژی جامعی برای مقابله با این مساله در جهت تضمین امنیت و دستیابی به منافع حیاتی خود می‌باشد.

مایلی و بهمنی (۱۳۹۱) در مقاله‌ای با عنوان «جنگ سرد نوین و رقابت بین قدرت‌های جهانی در فضای سایبری» به این مورد اشاره می نماید که امروزه در سایه فضای سایبر، رقابت و همکاری دولت‌ها شکل جدید یافته است، این پژوهش به دنبال بررسی، نقش فضای سایبر بر رقابت بین قدرت‌های جهانی در دوره جنگ سرد نوین است. نتایج حاصله گویای این مطلب می باشد که فضای سایبر در شکل قدرت و روابط را تغییر داده و قدرت عمل دولت را محدود کرده است و گروه‌های غیر دولتی را قدرتمند ساخته است و روابط بین قدرت‌های جهانی را از حالت دو سویه به چند سویه تبدیل نموده است.

۳- ظهور اینترنت و شکل‌گیری فضای سایبر

اینترنت، شبکه‌هایی از رایانه‌های به هم پیوسته است که از پروتکل اینترنتی استاندارد[1] برای خدمت‌رسانی به میلیاردها کاربر در سراسر جهان استفاده می‌کند. تا قبل از اواخر دهه ۱۹۸۰، اینترنت در اصل به منظور مبادله اطلاعات نظامی طراحی شده بود. اما در اواخر دهه ۱۹۸۰ وزارت دفاع آمریکا و بنیاد ملی علوم آمریکا، خصوصی‌سازی اینترنت را آغاز نموده‌اند. طولی نکشید که موسسات تجاری نیز اینترنت را تسخیر کردند و امکان دسترسی به اینترنت را برای جمع کثیری از کاربران تجاری و خصوصی مهیا ساختند. (Spar,1999:34)

[1] TCP/IP

فضای سایبر[1] یا فضای مجازی در تعریف برخی از نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی، بدون در نظر گرفتن جغرافیای فیزیکی». این فضا در واقع یک محیط است که ارتباطات در آن انجام می‌شود، نه صِرف مجموعه‌ای از ارتباطات. (مایلی‌و بهمنی،۱۳۹۱:۱۳۹) دپارتمان دفاعی ایالات متحده[2] ، فضای سایبر را به مثابه قلمروی جهانی در محیط اطلاعاتی تعریف می‌کند که مرکب از شبکهٔ هم‌بسته زیرساخت‌های فناوری اطلاعات، شامل: اینترنت، شبکه‌های ارتباط راه دور، سیستم‌های رایانه‌ای، پردازش‌گرها و کنترل کننده‌های تعبیه شده در آن می‌باشد. (Libicki,2009:6) این فضا از ویژگی گستردگی برخوردار است، چراکه برخلاف سایر حوزه‌های فیزیکی محدود نیست. ابزارهای قدرت در این فضا با عوامل متعددی شکل گرفته است. (Betz and Stevens,2011:34)

٤- قدرت سایبری و تاثیر آن بر حوزه‌های مختلف

مفهوم «قدرت سایبری» را می‌توان در برابر مفاهیمی چون «قدرت دریایی»، «قدرت هوایی»، قدرت زمینی» و حتی «قدرت فضایی» بررسی کرد. (Kramer,2009:4-5) دنیل کوهل۳، قدرت سایبری را به عنوان قابلیت و توانایی استفاده از فضای مجازی برای ایجاد مزیت‌ها و تاثیر بر رویدادها در سراسر محیط عملیاتی (زمین، دریا، هوا، فضا و فضای سایبری) و در تمام ابزارهای قدرت (دیپلماسی، اطلاعات، ارتش و اقتصاد) عنوان می‌کند. (Kuehl,2009:29) جوزف نای٤، نیز بیان می‌دارد: «قدرت سایبری وابسته به منابعی است که ویژگی‌های حوزه فضای سایبری را تعیین می‌نماید». او قدرت را در توانایی دست‌یابی به نتایج مورد انتظار از راه ابزارها و امکانات در فضای سایبری و دیگر حوزه‌ها معرفی می‌کند. (Nye,2011:8)

استار[5]، قدرت‌گیری بازیگران بین‌المللی را در عرصهٔ سایبر، مبتنی بر اهرم‌های قدرتی می‌داند که این عرصه ارائه می‌کند. از نظر او، اهرم‌های قدرت در قالب سیاسی، اقتصادی، نظامی و اطلاعاتی تعریف می‌شوند. سطح زیرین هرم، شامل زیرساخت‌هایی است که به فضای سایبر شکل می‌دهد. خروجی این زیرساخت‌ها، سطوح سنتی قدرت (سیاسی، اطلاعاتی، نظامی، و اقتصادی) را تقویت می‌کند. این سطوح قدرت، خود پایه‌هایی را برای توانمندسازی بازیگران در رأس هرم فراهم می‌کند. این بازیگران عبارتند از: افراد، تروریست‌ها، جنایت‌کاران

[1] cyberspace
[2] The Department of Defense (DOD)
[3] Daniel T. Kuehl
[4] Joseph Nye
[5] Stuart H. Starr

فراملی، شرکت‌ها، دولت–ملت‌ها و سازمان‌های بین‌المللی. این هرم، سویهٔ دیگری نیز دارد و آن «مسائل نهادی» است. این مسائل شامل عواملی چون حکومت، ملاحظات حقوقی و قانونی، نظم‌دهی، به‌اشتراک‌گذاری اطلاعات و ملاحظاتی درخصوص آزادی‌های مدنی است. (Stuart,2009:47)

تکنولوژی سایبر به‌طور روزافزونی در توانایی اقتصادی نیز نقش حیاتی ایفا می‌کند. در اقتصاد جهانی قرن بیست‌ویک، که اقتصادی جهان‌شمول و به‌هم‌پیوسته شده است، فضای سایبر را می‌توان تنها عامل مهم به‌هم–پیوستگی بازیگران با یکدیگر دانست که تولید را تقویت می‌کند، بازارهای جدیدی می‌گشاید و مدیریت ساختارهایی را که ثروت‌های کلانی ایجاد می‌کند ممکن می‌سازد. به‌لحاظ نظامی، توانمندی سایبری شاید مهم–ترین ابزار نوظهور چند دههٔ گذشته باشد. در حال حاضر اغلب کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. دکترین‌های جدید نظامی براساس فضای سایبر تدوین می‌شود. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ‌های متعارف، قدرت سایبر، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است و این توانمندی برپایهٔ تکنولوژی‌های مدرن شکل گرفته است. قدرت سایبر روزبه‌روز خود را به‌عنوان عاملی اثرگذار بر سیاست‌گذاری‌های ملی در تمام حوزه‌های اشاره‌شده توسعه می‌دهد. در زمینه‌های متعددی، از اقدامات ضدتروریستی گرفته تا سامان‌دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، ردپای توانمندی سایبر را می توان مشاهده کرد. در امور دولتی و حتی محلی، قدرت سایبر در شکل‌دهی به این موضوع که حکومت‌ها چگونه به شهروندان خود خدمات عمومی ارائه می‌کنند که حتی تا یک دهه پیش وجود نداشت، موضوعیت پیدا می‌کند. میزان تسهیل در دسترسی به این فضای تکنولوژیک، میزان موفقیت شهروندان و به‌تبع آن دولت را رقم می‌زند. توانمندی سایبری میان سایر عناصر و ابزارهای قدرت نیز پیوند برقرار می‌سازد و آنها را برای تغییر وضعیت به بهترین وضعیت یاری می‌رساند؛ به‌عبارت دیگر، فضای سایبر همانند مادهٔ خامی است که سوخت اقتصاد و جامعه را فراهم می‌کند. (زابلی‌زاده و وهاب‌پور،۱۳۹۷: ۷۱–۷۲)

۵– چالش‌های نوین امنیتی دولت–ملت در فضای سایبر

مقیاس نبردهای اطلاعاتی، امروزه کاملاً تغییر یافته و طیفی از نفوذ به شبکه رایانه‌ای دشمن، تا حتی تهاجم به سیستم‌های باوری و ارزشی دشمن را شامل می‌گردد. در واقع این کارکرد در عصر اطلاعات، معنای امنیت را که ورای تعریف ساده نظامی آن می‌باشد و برابر با تاثیرگذاری در عرصه نامحسوس عقاید و ارزش‌هاست، بازتاب

می‌دهد. آنچه توجه ما را به این تغییرات جلب می‌نماید آن است که مفهوم انقلاب اطلاعات و ارتباطات در بطن سازوکارهای تسلیحاتی، مفهوم راهبرد و نوع نبرد جای دارد و واقعیت آن است که فناوری اطلاعاتی کشورهای کمتر قدرت یافته، گروه‌های مشخص و حتی افراد را قادر نموده تا به سهولت به حمله یا ضدحمله بپردازند. حتی ابرقدرت‌هایی مانند آمریکا نیز در برابر چنین حملاتی آسیب پذیرند. (JaBae,2003:84)

فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصت‌های بسیار زیادی را برای یک کشور به وجود آورد، به همان میزان نیز می‌تواند تهدیدهای بزرگی را به همراه داشته باشد. تکنولوژی‌های اطلاعاتی در منابع، نوع و ابزارهای تهدید، تحولی شگرف ایجاد نموده‌اند. این تکنولوژی‌ها هم از لحاظ کمی (تعدد و تنوع منابع تهدید) و هم از لحاظ کیفی (پیچیده‌تر و کارآمد شدن ابزارهای سنتی تهدید)، ابزارهای تهدید امنیت ملی را متحول کرده است. در گذشته منابع تهدید امنیت دولت‌ها مشخص بود، اما امروزه چنین تعینی وجود ندارد. فناوری‌های نوین اطلاعاتی، تهدیدها و آسیب‌پذیری‌های امنیتی متعددی را متوجه کشورها اعم از بزرگ یا کوچک، پیشرفته یا در حال توسعه ساخته است. زیرا گسترش تکنولوژی‌های ارتباطی- اطلاعاتی، فاصله موضوعات داخلی و خارجی را محو کرده و افراد و جوامع را با تهدیدهای فراملی پیوند داده است. همچنین این تکنولوژی‌ها با خلق موجودیت-های بدون ساختار فیزیکی و مجازی و فارغ از محدودیت‌های طبیعی، نه تنها حاکمیت ملی را در برخورد با تهدیدهای امنیتی تضعیف نموده، بلکه قدرت تأثیرگذاری و عدم تعین تهدیدها را نیز افزایش داده است. (Chabinsky,2010:3)

گزارش مجمع جهانی اقتصاد (WEF) مخاطرات جهانی سال ۲۰۱۸، تهاجمات سایبری را پس از بلایای طبیعی و رویدادهای شدید آب و هوایی به عنوان اصلی‌ترین عامل آشوب و اختلال در پنج سال آینده معرفی کرد. این گزارش بیان می‌کند: «بدترین سناریو این است که مهاجمان بتوانند سیستم‌هایی را که عملکرد جوامع را حفظ می‌کنند از کار بیندازند». (محمدی،۱۳۹۷:۷)

با ظهور فضای مجازی، ظرفیتی استثنایی برای سلطه بر جهان به وجود آمده است که می‌توان آن را به «استعمار مجازی» یا «استعمار سوم» تعبیر نمود. (گوئو،۱۳۹۲:۲۵) در فضای مجازی، ما با تحول در مفاهیم پیشین قدرت و قبض و بسط آن مواجهیم. یعنی قدرت از حالت شخصی شدن، به حالت رسانه‌ای شدن سوق یافته که موجب حاکم شدن نگرش تعاملی-توافقی-رقابتی-تفاهمی بر نظام کنونی بین‌الملل شده و در عصر انقلاب اطلاعات و ارتباطات، مرزهای ملی رسوخ پذیر شده است. این روند ایجاد کشور مجازی و دولت مجازی و شیشه‌ای شدن

مرزها و جغرافیازدایی باعث شده تا عنصر گسترش اطلاعات، قدرت را به‌طور گسترده‌ای پخش نموده و شبکه-های غیررسمی به انحصارگری بوروکراسی‌های سنتی خاتمه دهند. (متقی و دیگران،۱۳۹۲:٤٨)

جهان دیجیتال، به سبب ارزانی و دسترسی گسترده به فناوری اطلاعاتی، توانمندی قابل‌ملاحظه‌ای حتی برای فقیرترین دولت‌ها و کنش‌گران منطقه‌ای و جهانی فراهم نموده است که ممکن است برای به‌چالش‌کشیدن و تهدید دیگران استفاده شود. این مسئله برخلاف فناوری‌های نظامی مهم عصر صنعتی است. در عصر اطلاعات، سخت‌افزارها و نرم‌افزارها به‌صورت گسترده در دسترس و به‌سادگی قابل استفاده است، درحالی‌که در سلاح‌های عصر صنعتی، مانند سلاح‌های هسته‌ای، موشک‌های قاره‌پیما، ناوهای جنگی هواپیمابر و تانک‌ها، این‌گونه نیست. بنابراین، در عصر اطلاعات، دولت‌ها تنها کنش‌گران بین‌المللی‌ای نیستند که ممکن است توانمندی‌های فنی را توسعه دهند تا برای آسیب‌رسانی استفاده کنند؛ بلکه شرکت‌های چندملیتی، سازمان‌های غیردولتی، گروه‌های جنایی و تروریستی و حتی افراد ممکن است در حوزه سایبر دست به عملکردهای جنگی بزنند. (آلبرتس و پاپ،۱۳۸۵:٤٥)

از این رو، امروزه به موازات فعالیت‌های نظامی، بهره‌برداری از فضای مجازی رو به گسترش، برای انجام حملات به زیرساخت‌ها و تاثیر بر ذهن انسان در حال انجام است. (Reynolds,2016:5) یکی از حوزه‌های مهم حیات بشری، هویت فردی، گروهی و ملی انسان‌ها و تاثیر آن بر روابط اجتماعی است. وجود هر نوع چالشی در بنیان‌های هویتی یک کشور، متاثر از فضای سایبر، می‌تواند تاثیرات بسیار زیادی بر فرایند سیاست-گذاری داخلی و خارجی گذاشته و آن را با چالش جدی روبه‌رو نماید. (نجفی و پوراحمدی، ۱۳۹۸:۱۵۷)

چالش‌های امنیتی در فضای سایبر را می‌توان حد نهایت معضلات کنونی دولت-ملت‌های مدرن دانست. البته این چالش‌های نوین مجازی در دوران معاصر علاوه بر دولت‌ها، بازیگران غیردولتی را نیز درگیر خود ساخته است . همان‌گونه که در جنگ‌های نظامی، سلاح‌های سخت‌افزاری، موجودیت دولت هدف را مورد حمله قرار می‌دادند؛ در جنگ سایبر نیز تکنولوژی‌های نوین رایانه‌ای، ماشین دولت، نهادهای مالی و زیرساخت‌های حیاتی در بخش‌های انرژی، حمل ونقل و در نهایت روحیه و عزم ملی را هدف حملات خود قرار می دهند. (Carr,2003:12)

در حوزه جنبش‌های اجتماعی متاثر از فضای سایبر نیز فضای جریان‌ها دارای اهمیت بیشتری از فضای مکان‌ها می‌باشد. هرچند بدون فضای مکان‌ها، سیاست همانند جزئی از زندگی انسانی ناممکن می‌گردد، اما در حوزه

فعالیت جنبش‌های اجتماعی، فضای جریان‌ها تعیین‌کننده‌ترین عنصر در سه حوزه اصلی جنبش یعنی حوزه آگاهی، حوزه هم‌بستگی و حوزه برساختن هویت است. (واعظی،۱۳۹۰: ۱۷٤-۱۷۵)

فضای سایبر شرایط جدیدی ایجاد نموده که در آن موضوعات روابط بین‌الملل نیز به شکلی متفاوت مطرح می‌شوند و در نتیجه شکل جدیدی از سیاست با عنوان «سایبر پلیتیک» ایجاد شده که پیامدهای ویژه‌ای در حوزه امنیت ملی و جهانی دارد. فضای تعامل سیاست و سایبر، یا به تعبیر درست‌تر فضای سایبرپلیتیک، جدیدترین و مهم‌ترین حوزه مورد توجه کارشناسان سیاست و روابط بین‌الملل در عرصه نظری و عملی محسوب می‌شود که غفلت از آن می‌تواند آسیب‌های جدی و غیرقابل پیش‌بینی برای کشورها به عنوان مهم‌ترین بازیگران در عرصه روابط بین‌الملل داشته باشد. سایبرپلیتیک مفهومی دو بخشی می‌باشد که اشاره به تعامل و پیوستگی دو عرصه سیاست (محل دوستی، همکاری، رقابت، ستیزه و جنگ بر سر ارزش‌ها و منافع) و اینترنت (فضایی جدید برای بازیگری) دارد. (عابدی،۱۳۹٤:۲)

در دوران کنونی، نرم‌افزارهای مخرب و ویرانگر و تهدید علیه امنیت داده‌ها و اطلاعات، تبدیل به فرآیندی پیچیده‌ای شده است. تنوع این حمله‌ها و تهدیدها سبب ایجاد انواع مختلف روش‌های دفاعی شده که صرف هزینه‌های فراوان را برای شرکت‌ها و سازمان‌های مختلف به وجود آورده است. با رشد فناوری‌های مربوط، مهاجمان این صنعت نیز با به‌کارگیری روش‌های نوین، اقدام به تولید بدافزارها و کدهای مخرب برای ناامن‌سازی این فضا نمودند. در این بین تولید بدافزارها به عنوان یکی از راه‌کارهای مخرب و قوی، همواره مورد توجه این مهاجمان و سازمان‌های پشتیبان آنها بوده است. در این میان جمهوری اسلامی ایران به عنوان محور مقابله با استکبار جهانی، همواره یکی از هدف‌های اصلی سازمان‌های اطلاعاتی غرب بوده است. (لرستانی،۱۳۹۷:۱۲۵)

یکی از بارزترین تهدیدات ناهم‌طراز در فضای مجازی، جنگ سایبری می‌باشد که هر سه ضلع مثلث دولت، ملت و ارتش را شامل می‌شود. (توکل،۱۳۸۵:۲٦) این نوع مقابله و جنگیدن ابعاد مختلفی را در بر می‌گیرد از جمله خرابکاری اینترنتی، جمع‌آوری داده‌ها با هدف دسترسی به اطلاعات طبقه‌بندی شده، ایجاد اخلال در سرویس‌دهی، ایجاد تغییر و اخلال در زیرساخت‌های حیاتی یک کشور. (Peterson,1996:99) جنگ در فضای مجازی را می‌توان در کنار جنگ دریایی، زمینی، هوایی و فضایی، پنجمین عرصه نبرد دانست. بنابراین می‌توان گفت اگرچه این جنگ در فضای مجازی با تکنولوژی‌های جدید رایانه‌ای رخ می‌دهد، اما روش‌ها و ابزارهایش چندان متفاوت از محیط متعارف نبرد نیست. (Chabinsky,2010:4) برخی از حملات سایبری،

هرچند خطرناک هستند، اما لزوماً به جنگ سایبر ختم نمی‌شوند. در واقع، تنها اقداماتی در این مقوله می‌گنجند که با انگیزه سیاسی و با هدف وارد آوردن ضربه جدی به زیرساخت‌های حیاتی یک بازیگر دولتی یا غیردولتی طراحی شده باشند. (Carr,2003:12)

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند. از یک سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های چالش‌های امنیتی نوین دولت–ملت‌ها در فضای سایبر در مؤلفه‌های زیر خلاصه می‌شود:

۱. **ابهام و نامشخص بودن فضای سایبر:** اقداماتی که در فضای سایبر یا عرصه مجازی درگیری، رخ می‌دهد از ماهیت نامشخصی برخوردار است. همین ماهیت مبهم، تأثیر چالش‌های امنیتی منبعث شده از فضای سایبر را بر زندگی واقعی و عرصه فیزیکی محیط سیاسی، اجتماعی و اقتصادی جوامع افزایش می‌دهد. (Glaessner,2004:9)

۲. **عدم پایبندی به چارچوب اخلاقی، ارزشی یا هنجاری:** یکی از مواردی که بر پیچیدگی اقدامات در فضای سایبر می‌افزاید، این نکته است که در این فضا نمی‌توان هیچ چارچوب اخلاقی، ارزشی یا هنجاری برای مبارزه و درگیری تعریف کرد. (Chang &Billo,2004:12)

۳. **دست‌یابی آسان به اطلاعات فرامرزی و جهانی با هزینه کم:** بارزترین ویژگی فضای سایبر، دسترس‌پذیر ساختن سریع و با حداقل هزینه همه اطلاعات «آنلاین[1]» است. از ویژگی‌های دیگر آن می‌توان به جهانی و فرامرزی بودن دست‌یابی آسان به آخرین اطلاعات را نام برد. (سلیمانی فارسانی،۱۳۸۸:۴۱)

٤. **تعدد بازیگران و پراکندگی قدرت در فضای سایبر:** هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا دستیابی نرم‌افزارهای مخرب به این معناست که تقریباً هر کسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته، گروه‌های تروریستی، شرکت‌های خصوصی و دولت–ملت هستند. (Charney,2009:5-6)

[1] On Line

۵. **هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام:** هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد. (Sharp & Lord,2011:20)

٦. **ناشناس ماندن بازیگران و عدم قابلیت ردیابی:** اینترنت به عنوان سیستم نامتمرکز طراحی شده و کاربران آن، غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. (Ibid,22)

۷. **تأثیرگذاری شگرف:** ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان‌ها شود. (Sharp & Lord,2011:22)

۸. **کمرنگ شدن نقش جغرافیا:** فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدیشان هستند. (Starr,2009:18)

۹. **ساختار فضای اینترنت:** اینترنت، دامنه مشترک و یکپارچه است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به از سوی دیگر، ساختار تهدید را بسیار دشوارتر کرده است. (Charney,2009:5-6)

۱۰. **پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری:** احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. در نتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه-های جایگزین غیر سایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند. (خلیلی‌پور رکن‌آبادی و نورعلی-وند،۱۳۹۱:۱۷۱)

٦- روش ها و ابزارهای نوین تهدید کننده امنیت دولت-ملت‌ها در فضای سایبر

فناوری‌های نوین اطلاعاتی در حوزه سایبر، در منابع، نوع و ابزارهای تهدید، تحولی بزرگ ایجاد نموده‌اند. این فناوری‌ها هم از لحاظ کمی و هم از لحاظ کیفی، ابزارهای تهدید امنیت ملی کشورها را متحول نموده‌اند. در گذشته منابع تهدید امنیت ملی دولت‌ها مشخص و تقریبا ثابت بوده استد، اما امروزه فناوری‌های نوین اطلاعاتی و ارتباطی، تهدیدها و آسیب‌پذیری‌های امنیتی متعددی را متوجه امنیت ملی کشورها اعم از بزرگ یا کوچک، پیشرفته یا در حال توسعه نموده است.

رشد جمعیت کاربران در جهان دیجیتالی بدون مرز، در عصری که ماشین‌های دیجیتال و کاربرانش تبدیل به جنگاوران سایبر شده‌اند، این امکان را به بازیگران دولتی و غیردولتی می‌دهد که میلیون‌ها یا شاید ده‌ها میلیون ماشین دیجیتال را تسخیر و کنترل کنند. (Libicki,2009:4) در این میان نوع ابزار جنگی به کار گرفته شده در فضای مجازی نیز بسته به بازیگری که آن را به کار می‌برد، از درجه اهمیت متفاوتی برخوردار است. مهمترین ابزارهای مورد استفاده در عملیات های سایبری را می‌توان در دو گروه «بدافزار[1]» و «باج افزار[2]» تقسیم‌بندی نمود.

- **بدافزار:** در اصطلاح کلی به نرم‌افزارهای مخرب مانند کرم‌ها، ویروس‌های رایانه‌ای، تروجان‌ها[3] و نرم‌افزارهای جاسوسی[4] گفته می‌شود که با هدف‌های مختلفی از جمله جمع‌آوری اطلاعات حساس، دسترسی به دستگاه‌های رایانه‌ای خصوصی و در برخی موارد تخریب سامانه‌ها در شکل‌های گوناگون طراحی شده و با کمک عوامل انسانی یا به صورت خودکار و به شیوه‌های خاص و رسانه‌های چندگانه در بین رایانه‌ها منتشر می‌شوند. (لرستانی،۱۲۹:۱۳۹۷)
- **باج‌افزار:** نیز خود نوعی بدافزار شامل یک مهاجم است که فایل‌های سیستم رایانه قربانی را قفل می‌کند. این کار معمولاً از طریق رمزگذاری صورت می‌گیرد و خواستار پرداخت پول برای رمزگشایی و باز کردن قفل آنها است. (پرهوده،٤:۱۳۹۸)

از مهمترین روش‌های مورد استفاده در عملیات‌های سایبری می‌توان به هکینگ و جاسوسی سایبری، مهندسی اجتماعی، فیشینگ و تروریسم سایبری اشاره نمود:

[1] Malware
[2] Ransomware
[3] Trojan
[4] Spyware

○ **هکینگ و جاسوسی سایبری:** در علوم سایبری، از نفوذ در خیلی از موارد به عنوان هک نامبرده شده و هکرها را به نفوذگران ترجمه کرده‌اند. به طور متعارف، هکر به شخصی اطلاق می‌شود که از دانش شبکه خود و سامانه‌های رایانه‌ای در جهت حصول دسترسی غیرمجاز به سیستم‌های رایانه‌ای، در جهت مرور اطلاعات، کپی، تعویض، حذف و یا نابودی آن بهره می‌گیرد. (زنجانی،۱۲:۱۳۹۸) جاسوسی سایبری اشاره به فعالیت‌های آگاهانه طراحی شده برای نفوذ به سیستم‌های کامپیوتری و یا شبکه‌های استفاده شده از سوی دشمن به منظور هک اطلاعات و یا انتقال از طریق این سیستم و یا شبکه‌های دیگر است. (فقیه حبیبی،۱۱۸:۱۳۹۵)

○ **مهندسی اجتماعی**[1]: سوء استفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است، که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند. مهاجم به جای استفاده از روش‌های معمول و مستقیم نفوذ جمع‌آوری اطلاعات و عبور از دیواره آتش[2]، برای دسترسی به سیستم‌های سازمان و پایگاه داده‌های آن، از مسیر انسان‌هایی که به این اطلاعات دسترسی دارند و با استفاده از تکنیک‌هایی برای فریب دادن آنها، به جمع‌آوری اطلاعات در راستای دست‌یابی به خواسته‌های خود اقدام می‌کند؛

○ **فیشینگ**[3]: نوعی کلاهبرداری که در آن ایمیل‌های جعلی ارسال می‌شود که شبیه ایمیل از منابع معتبر است. با این حال، هدف از این ایمیل‌ها سرقت داده‌های حساس مانند کارت اعتباری یا اطلاعات ورود به سیستم است. (پرهوده،٤:۱۳۹۸)

○ **تروریسم سایبری:** منظور از وجه مجازی تروریسم، وجهی از تروریسم است که در آن مولفه‌ای رایانه‌ای وجود دارد. امروزه سایبر تروریسم خطرناک‌تر از تروریسم سنتی است، این امر به دلیل رشد روزافزون ساختار اقتصادی و خدمات‌رسانی کشورهاست که مبتنی بر فناوری‌های اطلاعاتی و ارتباطی می‌باشد. (صدوقی،۳۱:۱۳۸۰)

۷- جمهوری اسلامی ایران و چالش‌های نوین امنیتی در فضای سایبر

جهانی شدن با شکل جدیدی که به محیط امنیتی، بازیگران و قواعد بازی امنیت خارجی داده است، سرمنشأ تهدیدهای کاملاً جدیدی برای جمهوری اسلامی ایران گردیده است که تا دهۀ پیش وجود نداشته است. مفهوم کلیدی در این رابطه، تهدید در فضای الکترونیکی و مجازی است که با جنگ‌های کلاسیک کاملاً متفاوت می-

[1] Social Engineering
[2] Firewall
[3] Phishing

باشند. امروزه امنیت سایبری از یک موضوع در حاشیه و تحت عنوان کلی زیرساخت حساس، به صدر تهدیدات امنیتی کشورها صعود نموده است. با ورود به عصر اطلاعات، کیفیت و شرایط جنگ‌ها از پیچیدگی مفهومی و روش اجرا برخوردار شده و لذا جنبه‌های نوینی از درگیری در فضای سایبر شکل گرفته است. جمهوری اسلامی ایران نیز به دلیل آنکه محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی‌شماری را دربر داشته است، همانند هر کشور دیگری نیازمند استراتژی جامعی برای مقابله با این مساله در جهت تضمین امنیت و دست‌یابی به منافع حیاتی خود می‌باشد. از این رو در طول یک دهه گذشته، همواره رویکرد دفاعی حفاظت از زیرساخت‌های حساس وابسته به شبکه را مدنظر داشته است. اولین گام‌های مؤثر در سازماندهی پدافند غیرعامل در حوزه مقابله با تهدیدات سایبری که بتواند طرح‌ریزی مناسب، برنامه‌ریزی لازم و اجرایی موفق، اثربخش و کارآمد را امکان‌پذیر نماید، تدوین یک راهبرد مناسب است.

در حال حاضر بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی جمهوری اسلامی ایران، در کلیه سطوح اعم از افراد، موسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز به این فضا منتقل و یا اساساً در این فضا شکل گرفته است. عمده فعالیت‌های رسانه‌ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب‌وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیری یافته و از میان شاخص‌های تعیین شده برای سنجش توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده است. از طرفی وجوه مختلف زندگی شهروندان به معنای واقعی با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی، و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را به مخاطره خواهد انداخت. (سازمان پدافند غیرعامل،۱۳۹٤:٤)

در طول یک دهه گذشته تهاجمات سایبری متعددی بر علیه زیرساخت‌های حیاتی جمهوری اسلامی ایران صورت گرفته و خسارت گسترده‌ای را به بار آورده است. از مهم‌ترین این تهاجمات می‌توان به حمله ویروس استاکس‌نت در سال ۲۰۱۰ به تاسیسات هسته‌ای ایران، حمله ویروس دوکو یا استاکس‌نت پسر به شرکت ارتباطات راه‌دور ایران و چند شرکت تولید تجهیزات الکترونیکی و اماکن میزبان مذاکرات هسته‌ای ایران، حمله ویروس شعله در سال ۲۰۱۲ میلادی، حمله ویروس وایپر در سال ۱۳۹۰ به سایت اینترنتی وزارت نفت ایران و

برخی شرکت‌های تابعه آن اشاره نمود. دشمنان جمهوری اسلامی ایران در کنار استفاده از انواع ویروس‌ها و بد افزارها جهت به بار آوردن خسارات فیزیکی در زیرساخت‌های حساس و حیاتی ایران، از روش‌های دیگری چون جاسوسی اینترنتی و سرقت اطلاعات حساس و حیاتی ایران، تشکیل کمپین‌های سیاسی ضد ایرانی در اینترنت، تحریک جامعه ایران به نافرمانی مدنی الکترونیک در فضای اینترنت، پیش‌برد دموکراسی دیجیتالی و تروریسم سایبری و تروریسم روانی نیز بهره‌برداری گسترده نموده‌اند.

جمهوری اسلامی ایران پس از حملات سایبری ایالات متحده آمریکا و اسرائیل به تأسیسات اتمی خود در سال ۲۰۱۰ میلادی، افزایش توان سایبری خود را جهت حفاظت از زیرساخت های حساس و حیاتی خود و همچنین جهت مقابله به مثل، به یکباره تا حد زیادی ارتقا داده است. کارشناسان بر این باورند که حمله استاکس‌نت به تاسیسات اتمی ایران به عنوان کاتالیزوری در جهت تقویت و گسترش توان سایبری ایران عمل نموده است. (https://p.dw.com/p/3VxB2)

مرکز تحقیقات استراتژیک بین‌المللی آمریکا[1] اخیرا طی گزارشی با تاکید بر این نکته که توان سایبری ایران دائما در حال افزایش است، تاکید کرد که توان سایبری ایران اکنون از بسیاری از کشورها بیشتر است. این مرکز در گزارش تحلیلی خود تاکید دارد که ایران اکنون توان سایبری خود را تبدیل به یک قدرت ملی نموده است. به طوری که با یک سیستم و سازمان دقیق اقداماتش را برنامه‌ریزی کرده و انجام می‌دهد. روزنامه «وال‌استریت» در گزارشی اذعان نموده است که کشور ایران در حوزه اقدامات سایبری یکی از ۱۰ قدرت بزرگ جهان به حساب می‌آید و این مسئله غربی‌ها را به شدت ترسانیده است. همچنین طبق گزارش مرکز دفاعی «دیفنس تک»[2]، با استناد به آمار دریافتی از سازمان اطلاعات آمریکا، ایران جزء پنج کشور دارای قوی‌ترین نیروی سایبری جهان است. هفته‌نامه نیوزویک هم هکرهای ایرانی را بهترین‌های جهان می خواند و ارتش سایبری ایران را خطری بزرگ‌تر از چین، روسیه و کره شمالی برای ایالات متحده آمریکا عنوان می‌نماید. همچنین، شرکت نرم افزاری «چک پوینت»[3]، یکی از گروه‌های هکری ایران را لشکری با ۹ جان، توصیف کرد. در همین حال، رئیس ارشد امور سایبری ارتش رژیم صهیونیستی هم در مورد قابلیت‌های سایبری ایران هشدار داده است. (آیان نیوز،۱۳۹۸: شناسه خبر ۲۹۹۵۵)

[1] Center for Strategic and International Studies (CSIS)
[2] Defense Tech
[3] Check Point

در سند راهبردی پدافند سایبری کشور ۱۳۹۳متعلق به قرارگاه پدافند سایبری، توسعه آمادگی دفاعی و بازدارندگی در مقابل تهدیدات سایبری از موضوعات اساسی راهبردی پدافند سایبری جمهوری اسلامی ایران عنوان شده است. در این سند در خصوص بازدارندگی سایبری این چنین آمده است: «دفاع به شیوه دشمن، نتیجه‌ای برای ما در برنخواهد داشت و لذا باید از روش‌های بومی و خودی در دفاع بهره جست و همچنین دفاع باید تمام جوانب مربوط به فضای به‌هم پیوسته و شبکه‌ای شده سایبری را دربر گیرد، به گونه‌ای که هیچ حلقه ضعیفی در زنجیره سرمایه‌های کشور وجود نداشته باشد. چنین دفاعی، دشمن را با درِ بسته مواجه نموده و انگیزه‌های وی را برای تهدید و حمله کاهش خواهد داد و در صورت اقدام، هزینه‌های سنگینی را به وی تحمیل خواهد کرد. (سازمان پدافند غیرعامل،۱۳۹۳: ۸-۹)

یکی از مهمترین اقدامات ایران در کنترل و مدیریت فضای سایبر تلاش در راستای ایجاد و عملیاتی نمودن «شبکه ملی اطلاعات» یا «اینترنت ملی» می‌باشد. به نظر می‌رسد این اقدام جمهوری اسلامی ایران مانعی بر کنترل آمریکا بر فضای مجازی بوده و آسیب‌پذیری جمهوری اسلامی ایران را در برابر حملات و جاسوسی‌های سایبری از سوی دیگر کشورها به خصوص ایالات متحده آمریکا و اسرائیل کاهش خواهد داد. (جوادی،۱۳۹۵:٤)

مهم‌ترین تهدیدات سایبری پیش‌روی امنیت ملی جمهوری اسلامی ایران به شرح ذیل می‌باشد:

- تشکیل قرارگاه فرماندهی سایبری توسط آمریکا و ناتو برای انجام اقدامات آفندی علیه برخی کشورها؛
- اشراف دشمن بر فضای اینترنت و سایبری دنیا اعم از شبکه، اطلاعات، مراکز نگهداری داده، تولیدکنندگانِ اصلی سخت‌افزارها و نرم‌افزارها و خدمات؛
- وجود توافقات ضد امنیتی اعلام نشده بین برخی کشورها علیه جمهوری اسلامی ایران در فضای سایبر؛
- امکان تعبیه حفره‌های امنیتی مخفی در تجهیزات فروخته شده به ایران توسط سازندگان مربوطه؛
- ممانعت از فروش برخی از سامانه‌های مرتبط با فضای سایبر، به بهانه تحریم‌های بین‌المللی به ایران؛
- رویکرد و استراتژی‌های تهاجمی دشمنان بر استفاده از توان سایبری خود بر علیه زیرساخت‌های حیاتی ایران که بر سایبر متکی می‌باشند؛
- اعمال حاکمیت دشمن با استفاده از فضای حقوق بین‌الملل سایبر بر شبکه‌های جهانی از قبیل اینترنت، شبکه‌های ماهواره‌ای و ... ؛
- فقدان نظام حقوق بین‌المللی در حوزه دفاع سایبری. (جلالی‌فراهانی و میررفیع،۱۳۹۸:۲۷۲)

۸- بازدارندگی سایبری در اسناد راهبردی جمهوری اسلامی ایران

بازدارندگی یکی از موضوعات اساسی در حوزه دفاعی-امنیتی هر کشور می‌باشد. از این رو تقویت و توسعه ادبیات راهبردی در حوزه بازدارندگی و به طور خاص در امنیت و دفاع سایبری به منظور بهره‌برداری سازمان‌های مسئول در حوزه سیاست‌های کلی فضای سایبر جمهوری اسلامی ایران، یکی از موضوعات پراهمیت و اساسی می‌باشد. کسب قدرت بازدارندگی یکی از عوامل موثر در دفاع سایبری می‌باشد.

هدف از راهبرد بازدارندگی، کاهش یا از بین بردن خطر حمله با افزایش هزینه‌ها است تا مهاجم را به این نتیجه رساند که هزینه‌های حمله بیش از منافع آن است. برای کاربست این راهبرد، داشتن دو نوع توانمندی بسیار حیاتی و کلیدی است. اولین توانمندی، داشتن قابلیت دفاعی مستحکم و قوی است که باعث شود مهاجم برای شروع حمله خود احتیاط بیشتری به خرج داده و تامل بیشتری کند. مورد دوم، توانمندی قابل ملاحظه اقدامات تلافی‌جویانه است. (زابلی‌زاده و وهاپ‌پور،۱۳۹۷:٦۸) رهبری نظام جمهوری اسلامی ایران در بازدید از دانشگاه افسری امام علی علیه‌السلام بیان می‌دارند: « ما امیدواریم با اراده و همت این جوانان برومند ارتش جمهوری اسلامی ایران، به اوج قدرت بازدارندگی و اعتلای حقیقی در مأموریت شرافت‌مندانه دفاع از میهن و ملت، نظام اسلامی و اسلام عزیز دست یابیم.». (ملایی و دیگران،۱۳۹۷:۲٤۲)

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

۹- نهادها و متولیان حوزه دفاع سایبری در جمهوری اسلامی ایران

- **سازمان پدافند غیرعامل:** سازمان پدافند غیرعامل جمهوری اسلامی ایران در سال ۱۳۸۲ زیر نظر ستادکل نیروهای مسلح تشکیل گردید. سیاست‌گذاری، هدایت، نظارت راهبردی و توسعه امنیت، ایمنی و پایداری فضای

تبادل اطلاعات کشور و پشتیبانی از برنامه دستگاه‌ها و بخش‌های زیرساختی در جهت کاهش آسیب در برابر تهدیدات و جنگ، از طریق ساماندهی و به کارگیری منابع و ظرفیت‌های ملی، از جمله وظایف سازمان پدافند غیر عامل در حوزه دفاع سایبر می باشد. (حسینی و ظریف منش،۱۳۹۲:٦۱)

○ **قرارگاه دفاع سایبری**: در سال ۱۳۹۰ به دستور ستاد کل نیروهای مسلح، سازمان پدافند غیر عامل جمهوری اسلامی ایران، مامور تشکیل قرارگاه دفاع سایبری گردید. (فقیهی،۱۳۸۹:٤۱) ضرورت و اهمیت صیانت از فضای سایبری در مقابل انواع تهدیدات و تهاجمات سایبری و به‌ویژه جنگ سایبری موجب گردید قرارگاه پدافند سایبری کشور با هدف تمرکز بر دفاع از زیرساخت‌های حیاتی و حساس و مهم کشور در مقابل انواع تهدیدات و تهاجمات سایبری ایجاد شود. قرارگاه پدافند سایبری کشور وظیفه صیانت از مرزهای سایبری کشور در حوزه نظامی و به‌ویژه در حوزه ایمن‌سازی زیرساخت‌های حیاتی و حساسِ واقع شده در فضای سایبری را برعهده دارد. (ملایی و دیگران،۱۳۹۷:۲۵۳)

○ **مرکز بررسی تهدیدات سایبری سپاه پاسداران انقلاب اسلامی**: سپاه پاسداران جمهوری اسلامی ایران در حوزه مقابله با تهدیدات سایبری به طور عمده از سال ۱۳۸٦ وارد این عرصه شده است و در همین راستا اقدام به تاسیس قرارگاه دفاع سایبری تحت عنوان «سازمان نبرد الکترونیک و دفاع سایبری سپاه» نمود. این نهاد نظامی، تشکیلات نسبتا منظمی برای فعالیت در فضای مجازی و سایبری در هر دو حوزه دفاعی و تهاجمی ایجاد کرده است. این سازمان از سال ۱۳۹۳ تحت عنوان «فرماندهی امنیت سایبری سپاه» به فعالیت خود ادامه داده است. (شریعت‌پناه،۱۳۸۹:۱٦)

○ **پلیس فضای تولید و تبادل اطلاعات (پلیس فتا)**: نیروی انتظامی جمهوری اسلامی ایران در سال ۱۳۸۹ اقدام به تشکیل پلیس سایبری برای مبارزه با «جاسوسی، خرابکاری و نقض حریم خصوصی» نمود. ایجاد امنیت و کاهش مخاطرات برای فعالیت‌های علمی، اقتصادی، اجتماعی در جامعه اطلاعاتی، حفاظت و صیانت از هویت دینی و ملّی، مراقبت و پایش از فضای تولید و تبادل اطلاعات برای پیش‌گیری از تبدیل شدن این فضا به بستری برای انجام هماهنگی‌ها و عملیات برای انجام و تحقّق فعالیت‌های غیرقانونی و ممانعت از تعرض به ارزش‌ها و هنجارهای جامعه ایران در فضای مجازی، از جمله وظایف و مأموریت‌های پلیس فضای تولید و تبادل اطّلاعات نیروی انتظامی است. (www.syberpolice.ir)

○ **شورای عالی فضای مجازی:** حضرت آیت‌الله خامنه‌ای، در تاریخ هفدهم اسفند ۱۳۹۰ دستور تشکیل شورای عالی فضای مجازی به ریاست رئیس‌جمهور را صادر نمودند. در این دستور آمده است: «گسترش فزاینده فناوری‌های اطلاعاتی و ارتباطاتی شبکه جهانی اینترنت و آثار چشم‌گیر آن در ابعاد زندگی فردی و اجتماعی و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطه کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به‌وجود آید. از این رو شورای عالی فضای مجازی کشور با اختیارات کافی به ریاست رئیس جمهور تشکیل گردید. (حسینی و ظریف منش،۱۳۹۲:٦١)

۱۰- پیشنهاد و راه‌کار در راستای مدیریت بهینه فضای سایبر جمهوری اسلامی ایران

حوادث و پیامدهای یک دهه گذشته جمهوری اسلامی ایران، اشاره به این واقعیت دارد که بخش عمده‌ای از تهدیدهات بر علیه این کشور، به ویژه در سامانه‌ها، زیرساخت‌های حیاتی، یا مستقیماً از فضای سایبر نشأت گرفته‌اند و یا این فضا را هدف تهدید مستقیم خود قرار داده‌اند. از این رو، با توجه به خطرات و آسیب‌پذیری-های ذاتی موجود در فضای سایبری و روند رو به رشد بهره برداری از این فضا توسط آحاد جامعه، ریسک بهره-برداری از سامانه‌های مبتنی بر فناوری اطلاعات، که برای اقتصاد کشور حیاتی می‌باشند، را روز به روز افزایش داده است. پیچیدگی روز افزون و رو به ازدیاد سامانه‌ها و شبکه‌های مبتنی بر فناوری سایبر، چالش‌های امنیتی را برای جمهوری اسلامی ایران دربر داشته است.

از آنجایی که کنش و واکنش در عرصه سایبر، ادامه سیاست با ابزار دیجیتال است، لذا تنها با اتخاذ سیاست‌های هوشمندانه می‌توان آن را کنترل و مدیریت نمود. عملیات و تهاجمات سایبری دیگر کشورها و حتی بازیگران غیر دولتی به‌شدت تهدیدگر منافع و زیرساخت‌های حیاتی جمهوری اسلامی ایران است. از این‌رو، با توجه به آنکه اخیراً در دکترین نظامی ایران، «تهاجم سایبری» در کنار «دفاع سایبری» از اهمیت خاصی برخوردار شده است، ضروریست جهت مقابله با حملات سایبری، بومی‌سازی و مقاوم‌سازی زیرساخت‌های سایبری تأسیسات، صنایع راهبردی و خدمات عمومی، مورد توجه ویژه قرار گیرد. از این‌رو، با توجه به پیچیدگی‌های فناوری‌های مرتبط با فضای سایبری، اساسی‌ترین راهبرد برای حفظ امنیت و منافع ملی جمهوری اسلامی ایران در فضای سایبر، سرمایه‌گذاری گسترده در حوزه فناوری‌های سایبری اعم از ساخت تجهیزات و آموزش نیروهای متخصص در

کنار باز تعریفی جدید از اهداف، روش‌ها و ابزارهای مورد استفاده در تلازم با محیط سیاسی برای مقابله با ابهام، پیچیدگی و پویایی تهدیدهای امنیتی در فضای سایبر می‌باشد. در جهت کسب موفقیت در استراتژی‌های دفاع سایبری، متخصصان سایبری جمهوری اسلامی ایران می‌بایست، شناخت کافی از اهداف، ابزارها، تکنیک‌ها و تاکتیک‌ها مورد استفاده توسط دشمن در فضای سایبر داشته باشند.

با توجه به اینکه حملات سایبری در یک محیط بسیار پیچیده، سیستماتیک، متغیر، مبهم و غیر قابل کنترل رخ می‌دهد. بنابراین مدیریت آن نیازمند تدوین یک استراتژی امنیت ملی است. در همین زمینه دولت جمهوری اسلامی ایران باید بکوشد تا حد امکان قدرت سایبری خود را نیز متناسب با تکنولوژی‌های روز سایبری دنیا افزایش دهد. زیرا افزایش قدرت سایبری، کلید موفقیت سیاست‌های ایران برای مدیریت فضای سایبر و مبارزه و خنثی‌سازی اقدامات و حملات سایبری دشمنان این کشور محسوب می‌گردد. امروزه برای پیروزی در عرصه سایبر به عنوان پنجمین عرصه نبرد، تنها در اختیار داشتن تکنولوژی به همراه ارزش‌ها و هنجارهای اخلاقی-سیاسی می‌تواند حرف نهایی را بزند.

نتیجه گیری

امروزه اینترنت علاوه بر اینکه فضای جدیدی را برای همکاری و تعامل میان تمامی بازیگران ازجمله دولت‌ها، افراد، سازمان‌ها و نهادهای مختلف با سرعت و دقت بالا ایجاد نموده است، کمک فراوانی نیز به تسهیل و توسعه دسترسی به اطلاعات و دانش در عرصه ملی و بین‌المللی نموده است. قدرت سایبری می‌تواند بر حوزه‌های قدرت نظامی اعم از قدرت دریایی، هوایی، زمینی و فضایی و در عرصه قدرت اقتصادی و تجاری و غیره به طور کامل و هم‌زمان اثرگذار بوده و باعث تقویت این حوزه‌ها گردد. اما این فضا به همان نسبت که می‌تواند فرصت-های بسیار زیادی را برای کشورها به ارمغان آورد، به همان میزان نیز می‌تواند هم از لحاظ کمی و هم از لحاظ کیفی، تهدیدهای بزرگی را برای بخش‌های مختلف یک کشور ایجاد نماید.

تکنولوژی سایبر با خلق موجودیت‌های بدون ساختار فیزیکی و مجازی و فارغ از محدودیت‌های طبیعی، تعدد بازیگران و ناشناس بودن آنها، پراکندگی قدرت و عدم پایبندی به اصول اخلاقی و ارزشی و از همه مهم‌تر تاثیرگذاری شگرف، نه تنها حاکمیت ملی کشورها را در برخورد با خطرات و تهدیدات این حوزه تضعیف نموده است، بلکه قدرت تأثیرگذاری این تهدیدها را نیز افزایش داده است. امروزه جنگ در فضای سایبر را می‌توان در کنار جنگ دریایی، زمینی، هوایی و فضایی، پنجمین عرصه نوظهور نبرد دانست که قدرت نسبی دولت‌ها را و به-

تبع آن، بقای آنان را در نظام بین‌الملل متأثر می‌سازد. به گونه‌ای که امروزه کشورها برای تأمین امنیت ملی خود، مفهوم دفاع در جنگ‌های سنتی را با مفهوم نرم‌افزاری آن در فضای سایبری تلفیق نموده و در راستای دفاع از موجودیت خود گام برداشته‌اند. اگرچه جنگ سایبر معمولاً بین دولت‌ها با انگیزه سیاسی رخ می‌دهد اما این جنگ می‌تواند از طریق روش‌های متفاوت، بازیگران غیردولتی را نیز درگیر کند.

محیط سایبر به سرعت در حال تغییر است. این تغییرات و سیال بودن فضای سایبر، چالش بسیار بزرگی را برای کشورهای فعال در این عرصه به وجود آورده است. امروزه فعالیت در این فضا برای همه کشورها هم تهدید و هم فرصت تلقی می‌شود. تهدید برای کشورها و بازیگرانی که روزبه‌روز زندگی خود را بیشتر با فضای جدید پیوند می‌زنند و فرصت برای بازیگرانی که از امکان ضربه‌زدن یا برآورده‌سازی خواسته‌ها و منافع خود در شکل سنتی عاجز هستند یا تمایل ندارند هزینه‌های تهدید سنتی یک بازیگر دیگر را به جان بخرند. همه این موارد دست به دست هم داده است تا لزوم اتخاذ یک چارچوب سیاسی بین‌المللی برای مقابله با چالش‌های فضای سایبر، امروزه یکی از اولویت‌های اصلی امنیت ملی کشورهای جهان محسوب می شود.

جمهوری اسلامی ایران یکی از کشورهایی است که در طول یک دهه گذشته طعم تلخ خرابی و خسارات ناشی از حملات سایبری به خصوص از جانب ایالات متحده آمریکا و اسرائیل بر علیه زیرساخت‌های حساس و حیاتی خود را چشیده است. این کشور بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی خود را در کلیه سطوح اعم از افراد، موسسات غیر دولتی و نهادهای دولتی و حاکمیتی در فضای سایبر انجام می‌دهد. امروزه امنیت سایبری جمهوری اسلامی ایران از یک موضوع در حاشیه، به صدر تهدیدات امنیتی این کشور صعود نموده است. از این رو، این کشور در طول یک دهه گذشته، همواره رویکرد دفاعی حفاظت از زیرساخت‌های حساس وابسته به شبکه را مدنظر داشته و در راهبرد دفاعی خود نیز جایگاه والایی برای موضوع بازدارندگی در حوزه سایبر جهت منصرف نمودن متخاصمین از حمله به سرمایه ها و منافع ملی خود و در مقابل موجبات ارتقاء و تداوم پایداری زیرساخت‌های حیاتی خود قائل شده است.

منابع

آلبرتس، دیوید و دانیل، پاپ (۱۳۸۵). گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات، ترجمهٔ علی علی‌آبادی و رضا نخجوانی، تهران: پژوهشکدهٔ مطالعات راهبردی

صدوقی، مرادعلی (۱۳۸۰). فناوری‌های اطلاعاتی و حاکمیت ملی، تهران: دفتر مطالعات سیاسی و بین‌المللی

کاستلز، مانوئل (۱۳۹۳). قدرت ارتباطات، ترجمه حسین بصیریان جهرمی، تهران: پژوهشگاه فرهنگ هنر و ارتباطات

گوئو، چن بائو (۱۳۹۲). رسانه سلطه، سلطه رسانه، ترجمه فریده پیشوایی، تهران: کتاب نشر

متقی، افشین؛ زادگان، امیرحسین؛ امینی، حسن (۱۳۹۲). فضای سایبر، ژئوپلیتیک و قدرت هوشمند از منظر پدافند غیرعامل، تهران: سازمان انتشارات جهاد دانشگاهی

واعظی، محمود (۱۳۹۰). بحران‌های سیاسی و جنبش‌های اجتماعی در خاورمیانه، تهران: دفتر مطالعات سیاسی و بین‌المللی

توکل، اکبر (۱۳۸۵)، «مفهوم جنگ سایبری و کاربرد آن در جنگ آینده». فصلنامه علوم و فنون نظامی، سال سوم، شماره ۷، صص ۱۵-۳٤

جلالی فراهانی، غلامرضا و میررفیع،سید علی (۱۳۹۸)، «ارائه راهبردهای پدافند غیر عامل کشور در برابر تهدیدات سایبری». فصلنامه مطالعات دفاعی استراتژیک، سال هفدهم، شماره ۷۵، صص ۲۵۹-۲۸۲

حسینی، پرویز و ظریف‌منش، حسین (۱۳۹۲)، «مطالعه تطبیقی ساختار دفاع سایبری کشورها». فصلنامه پژوهش‌های حفاظتی-امنیتی دانشگاه جامع امام حسین، سال دوم، شماره ۵، صص ٤۱-٦۸

خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱)، «تهدیدات سایبری و تاثیر آن بر امنیت ملی». فصلنامه مطالعات راهبردی، سال پانزدهم، شماره دوم، صص ۱٦۷-۱۹٦

دیوسالار، عبدالرسول(۱۳۹۳)، «قدرت ارتباطات یا قدرت اطلاعات؛ نقدی بر نظریه قدرت شبکه‌ای مانوئل کاستلز». فصلنامه نقد کتاب؛ اطلاع رسانی و ارتباطات، سال اول، شماره ۳ و ٤، صص ۹۱-۱۱۰

زابلی‌زاده، اردشیر و وهاب‌پور، پیمان (۱۳۹۷)، «قدرت بازدارندگی در فضای سایبر». دو فصلنامه علمی پژوهشی، سال هشتم، شماره اول، صص ٤۷-۹۷

سازمان پدافند غیر عامل (۱۳۹۳)،«اصول حاکم بر پدافند سایبری و اهداف کلان در افق چشم انداز قرارگاه پدافند سایبری کشور»، ماهنامه پاپسا، شماره دوم، صص ۱-٤۰

سازمان پدافند غیر عامل (۱۳۹٤)،«مامورت، اهداف و رسالت پدافند سایبری»، ماهنامه پاپسا، شماره نهم، صص ۱-۳٦

سلیمانی فارسانی، امین (۱۳۸۸)، «انقلاب اسلامی و جنگ نرم». نشریه پیام انقلاب، شماره ۳۱

شریعت‌پناه، علی (۱۳۸۹)، «تهاجم و تقابل در فضای سایبری». ماهنامه پیام انقلاب، شماره ۳٦، صص ۱٦-۲۰

عسگرخانی، ابومحمد؛ قربانی، فاطمه و حلال‌خور، مهرداد (۱۳۹۳)، «نقش رسانه‌های اجتماعی جدید و شبکه‌سازی در انقلاب ۲۵ ژانویه مصرو بحران‌های پس از آن». فصلنامه پژوهش‌های راهبردی سیاست، سال سوم، شماره ۱۰، صص ۸۰-۱۱۲

عظیمی، فاطمه و خوشنودی، هادی (۱۳۹۵)، «نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن». فصلنامه مطالعات سیاسی، سال نهم، شماره ۳٤، صص ۱۵۹-۱۷۲

فقیه حبیبی، علی (۱۳۹۵)، « جنگ مدرن و تخاصمات سایبری در چارچوب فضای بین‌الملل». جستارهای سیاسی معاصر، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هفتم، شماره اول، صص ۱۱۵-۱٤٤

فقیهی، معصومه (۱۳۸۹)، «تهدیدات ارتباط منسجمی با فناوری دارند». ماهنامه دنیای مخابرات و ارتباطات، سال هفتم، شماره ۷۲، صص ٤۱-٤۷

لرستانی، علیرضا (۱۳۹۷)، «مروری بر روش‌های مقابله با بدافزارها و نرم افزارهای جاسوسی». فصلنامه مطالعات حفاظت و امنیت انتظامی، سال سیزدهم، شماره ٤۹، صص ۱۲۵-۱۵۲

مایلی، محمدرضا و بهمنی، محمد سعید (۱۳۹۱)، «جنگ سرد نوین و رقابت بین قدرت‌های جهانی در فضای سایبر». پژوهشنامه مطالعات روابط بین‌الملل، شماره ۲۰، صص ۱۳۳-۱٦۲

محمدی، ناصر (۱۳۹۷)، «تدوین قوانین جنگ سایبری». خبرنامه آفتا، شماره ۳۰، صص ۱-۲٦

زنجانی، جواد (۱۳۹۸)، «شناسایی و مقابله با تهدیدات سایبری رژیم صهیونیستی علیه ارتش جمهوری اسلامی ایران»، پایان‌نامه کارشناسی ارشد، دانشکده فرماندهی و ستاد ارتش جمهوری اسلامی ایران،

سایت‌های اینترنتی

آیان نیوز (۱۳۹۸)، « آمریکا شوکه شود/ آیا ایران مسئول هک بانک‌های آمریکایی و سریال بازی تاج و تخت بوده است؟» کد خبر: ۲۹۹۵۵، قابل دسترس در: http://www.ayannews.ir/ShowNews/29955

پرهوده، لیلا (۱۳۹۸)، «امنیت سایبری چیست؟». قابل دسترس در: https://www.nexterafactory.com/cyber-security

جوادی، محمود (۱۳۹۵)، «درس‌های راهبرد جدید سایبری آمریکا برای ایران». شورای راهبردی روابط خارجی، قابل دسترس در: https://www.scfr.ir/fa/14864/300

دویچه وله فارسی (۲۰۱۹)، «ابعاد احتمالی جنگ سایبری میان ایران و آمریکا». قابل دسترس در: https://p.dw.com/p/3VxB2

عابدی، سجاد (۱۳۹٤)، «تأثیر سایبرپلیتیک بر سیاست عملی و نظریه‌های روابط بین‌الملل». مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، قابل دسترس در: https://tisri.org/?id=3whsrs8j

منابع لاتین

Bell, David. (2007). Cyberculture Theorists: Manuel Castells and Donna Haraway. Routledge

Betz, J. David and Tim Stevens (2011), Cyberspace and the State: Toward a Strategy for CyberPower, London: The International Institute for Strategic Studies (IISS)

Carr, C. (2003). The Lessons of Terror: A History of Warfare Against Civilians. New York: Random House Trade Paperback

Chabinsky, S. R. (2010). “The Cyber Threat: Who’s Doing What to Whom?” Retrieved from Walter E Washington Convention Center: <http://fose.com/events/fose-2010/sessions/wednesday/chabinsky.aspx>

Chang, Welton & Billo, Charles (2004). Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States. Retrieved from Institute for Security Technology Studies at Dartmouth College: <www.ists.dartmouth.edu/docs/execsum.pdf

Charney, Scott (2009). "Rethinking the Cyber Threat A Framework and Path Forward", Microsoft Corp.

Glaessner, T. C. (2004). Electronic Safety and Soundness: Securing Finance in a New Age. World Bank Working Paper (26)

JaBae,Young (2003) Information Technology and The Empowerment of New Actors in International Relations,Journal of International and Area Studies,Volume.10,Number 2

Kuehl, D, (2009), From cyberspace to cyberpower: defining the problem, in: F. Kramer, S. Starr, L. Wentz (Eds.), Cyberpower and National Security, Potomac Books, Dulles, Virginia

Libicki, Martin C. (2009). Cyberdeterrence and cyberwar. USA: RAND Corporation

Lord, Kristin M. & Sharp, Travis (2011). "America's Cyber Future Security and Prosperity in the Information Age", Center for a New American Security, Volume I.

Nye, joseph (2011), The Future of Power, Public Affairs, Philadelphia, Pennsylvania

Peterson, John.(1996). Information Warfare: The Future, in Cyberwar: Security Strategy and Conflict in the Information Age. A lan D. Capen, Douglas H. Dearth, and Thomas Gooden, eds. AFCEA, International Press, Fairfax, VA.

Spar, Debora L (1999). "Lost in (Cyber) Space: The Private Role of Online Commerce," In A. Claire Cutler, Virginia Haufler, and Tony Porter. Albany (eds.), Private Authority and International Affairs, NY: State University of New York Press

Stuart, H(2009), "Developing a Theory of Cyber Power", in: F. D. Kramer, S. Starr, and L. K. Wentz (ed.), Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity