فضای سایبر و شیوه‌های نوین درگیری ایالات متحده امریکا با جمهوری اسلامی ایران

مهسا ماه‌پیشانیان ❋

چکیده

با ورود به عصر اطلاعات، کیفیت و شرایط جنگ‌ها از پیچیدگی مفهومی و روشی بسیار زیادی برخوردار شده و جنبه‌های نوینی از درگیری در فضای سایبر شکل گرفته است. جنگ سایبری مجموعه‌ای از فنون عملیاتی جدید و سبک نوینی از جنگ است که در مناقشه‌هایی در بالاترین سطح شدت به منظور هدف قرار دادن مخالفان به‌کار می‌رود. این جنگ شکل جدیدی از جنگ فرماندهی و کنترل است که کمتر به جغرافیا بستگی دارد بلکه بیشتر به ماهیت فضای شبکه‌های الکترونیک مربوط می‌شود. جنگ سایبر با هدف اختلال، آسیب‌زدن یا تغییر آنچه جمعیت هدف فکر می‌کنند با تمرکز بر روی افکارعمومی، نخبگان و یا هر دو به انجام می‌رسد. ایالات متحده امریکا با استفاده از قابلیت‌های فضای سایبر کوشیده است ابعاد نوینی از جنگ نرم بر ضد کشورمان را در این فضا شکل دهد. با توجه به اهمیت این جنبه نوین درگیری، متن حاضر به بررسی مشخصات اصلی جنگ سایبر به عنوان یک محیط استراتژیک پرداخته است و از طریق بررسی ماهیت، اهداف، ابزار و روش‌های حملات در فضای مجازی واکنش‌های دفاعی مناسب در برابر این حملات را نیز مورد تحلیل قرار می‌دهد.

واژگان کلیدی

فضای سایبر، جنگ سایبر، جاسوسی سایبر، تروریسم سایبری

❋. عضو هیئت علمی دانشگاه آزاد اسلامی واحد بوشهر

مقدمه

در سال‌های اخیر حکومت‌ها و سازمان‌های بین‌المللی با امنیت سایبر و لزوم توجه بسیار زیاد به این مقوله روبرو شده‌اند. چالش‌های امنیتی در فضای سایبر را می‌توان حد نهایت معضلات کنونی دولت‌های 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، حمل‌ونقل و در نهایت روحیه و عزم ملی را هدف حملات خود قرار می‌دهند. (Carr, 2003: 12)

اگرچه حملاتی که با انگیزه سیاسی در فضای سایبر علیه دولتی رخ می‌دهد در مقوله جنگ‌های سایبر قرار می‌گیرد، اما توجه به این نکته مهم ضروری است که همه این حملات با هدف سیاسی در فضای مجازی سازماندهی نمی‌شود. چنین حملاتی که معمولاً با انگیزه‌های اقتصادی یا شخصی صورت می‌پذیرند، در تحلیل نهایی جزو جنگ سایبر به‌حساب نمی‌آیند. بر همین اساس، درک تمایز بین اقدامات جنگی و غیرجنگی در فضای سایبر از اهمیت بسیار زیادی برای تدوین استراتژی‌های مناسب به‌منظور مقابله با این حملات برخوردار است. (Clarke & Knake, 2010: 146)

نکته مهم دیگر در مورد جنگ‌های سایبر این است که نوع ابزار جنگی به‌کار گرفته شده در فضای مجازی، بسته به بازیگری که آن را به‌کار می‌برد، از درجه اهمیت متفاوتی برخوردار است. برخی 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، همچون حملات سایبر گروه‌های تروریستی، جاسوسان و مجرمان سازمان‌یافته. (Rattray, 2001)

نکته دیگری که می‌توان در مورد جنگ سایبر گفت این است که امکان دارد یک دشمن

در به‌کار بردن وسایل متعارف جنگ سخت ناتوان بوده اما از چابکی و توانمندی بسیار زیادی برای ایجاد حملات سایبری برخوردار باشد. علاوه بر این، آنچه امروزه توانسته چهره جنگ سایبر را از جنگ‌های متعارف متمایز کند، سرعت و پیچیدگی ماهیت تهدیدها در فضای مجازی می‌باشد؛ به‌گونه‌ای که بازیگری که مورد حمله قرار گرفته باشد از سرعت بسیار زیاد و ماهیت پیچیده تهدیدها دچار غافلگیری شده و نمی‌تواند به‌صورت مناسب واکنش نشان دهد. همین مسئله سبب شده است که مفهوم پیروزی و شکست در جنگ سایبر از جنگ‌های متعارف متفاوت باشد. (Schaap, 2009: 135)

مسئله دیگری که بر شدت پیچیدگی جنگ در فضای سایبر می‌افزاید، این نکته است که در این فضا نمی‌توان هیچ چارچوب اخلاقی، ارزشی یا هنجاری برای مبارزه و درگیری تعریف کرد. بنابراین به نسبت ابهام و نامشخص بودن فضای سایبر درجه آسیب‌پذیری بازیگران نیز افزایش می‌یابد. (Billo & Chang, 2004: 12)

در کل در تعریف جنگ سایبر می‌توان گفت این جنگ زیرمجموعه‌ای از «جنگ اطلاعاتی[1]» است و شامل اقداماتی می‌شود که در فضای سایبر رخ می‌دهد. بنابراین، می‌توان جنگ سایبر را یک داستان نامتعارف هشداردهنده دانست که معمولاً بیشتر از آنچه که ارتباط نزدیکی با سیاست عمومی داشته باشد با فضای مجازی تکنولوژی مرتبط می‌باشد. (Krebs, 2009)

برای تحلیل صحیح از اهداف، ابزار و روش‌های جنگ سایبر، ابتدا باید به نکات ذیل در مورد مفهوم آن توجه کنیم:

ـ فضای سایبر که ارتباطات دیجیتال جهانی و ساختارهای انتقال اطلاعات را دربرمی‌گیرد، سبب شکل گرفتن چالش‌های امنیتی گسترده برای اشخاص، شرکت‌های بازرگانی، حکومت‌ها و سازمان‌های بین‌المللی شده است. البته امنیت سایبر در سال‌های اخیر بیشتر در حوزه سیاست عمومی و رسانه‌ای مطرح شده است؛

ـ اگرچه جنگ سایبر معمولاً بین دولت‌ها با انگیزه سیاسی رخ می‌دهد اما این جنگ

1. Information Warfare (IW)

می‌تواند از طریق روش‌های متفاوت، بازیگران غیردولتی را نیز درگیر کند؛

ـ در جنگ سایبر شناسایی اهداف نیز بسیار مشکل است. اهداف این جنگ می‌تواند دارای ابعاد سیاسی، نظامی، اقتصادی، صنعتی و مدنی باشد؛

ـ جنگ سایبر می‌تواند بازیگران این عرصه را برای دستیابی به اهداف سیاسی و استراتژیکی آنها بدون نیاز به جنگ مسلحانه توانمند سازد؛

ـ جنگ سایبر قدرت نامتناسبی را به بازیگران کم‌اهمیت و کوچک فضای سیاسی و اقتصادی می‌دهد؛

ـ در فضای سایبر حمله‌کنندگان می‌توانند بدون ترس از شناخته شدن یا حتی مجازات به اهداف خود دست یابند؛

ـ در جنگ سایبر مرز بین اقدامات نظامی و غیرنظامی مبهم بوده و حملات سایبر می‌تواند به‌وسیله بازیگران دولتی یا غیردولتی یا حامیان آنها طراحی شود؛

ـ 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؛

ـ اهداف و ابزار جنگ سایبری برای موفقیت باید با دیگر روش‌های اجبار، اقناع و درگیری همراه شود؛

ـ در جنگ سایبر اهداف سیاسی، فرهنگی، اقتصادی و اجتماعی به‌طور متناقضی با اهداف امنیتی دنبال می‌شود. بر همین اساس باید در محیط سیاسی، چارچوب استراتژیک مناسبی برای مقابله با این حملات تدوین شود. یعنی برای جنگ سایبر باید الزامات اخلاقی، قانونی، ارزشی و هنجاری معین تدوین شود. (Chabinsky, 2010)

حال با توجه به این مقدمه، در ادامه به بررسی این سؤالات مهم خواهیم پرداخت که:

ـ آیا تکنولوژی‌های اطلاعاتی و شبکه‌های اجتماعی مجازی برای امنیت ملی فرصت‌ساز

است یا تهدیدزا؟

ـ آیا تکنولوژی‌های نوین اطلاعاتی سبب از میان رفتن اهمیت مرزهای جغرافیای در جهان معاصر شده است؟

ـ آیا تکنولوژی‌های نوین اطلاعاتی با زمینه‌سازی برای دزدیده شدن اطلاعات مهم و حیاتی یک کشور باعث عدم‌احساس امنیت در میان مردم می‌شوند؟

در پاسخ به همه این سؤالات می‌توان تنها به یک نکته اکتفا کرد و آن اینکه جنگ سایبر، مهم‌ترین تهدید برای امنیت ملی و بین‌المللی در دنیای کنونی است.

تهدیدها و چالش‌های امنیتی در جنگ‌های سایبر

حکومت، بخش خصوصی و شهروندان، همگی از جانب بازیگران دولتی یا غیردولتی، مجرمان سازمان‌یافته و گروه‌های تروریستی هستند. علی‌رغم رشد آگاهی و شناخت جهانی از فضای سایبر، ماهیت، نوع، ابزار، تکنیک‌ها و تاکتیک‌های حملات در جهان مجازی همچنان ناشناخته باقی مانده است. (Shachtman, 2011) ماهیت تهدیدها در جنگ‌های سایبر برخلاف جنگ‌های سخت‌افزاری مبهم و نامشخص هستند. در این فضا شناسایی ماهیت و انگیزه بازیگرانی که تنها با هدف مجرمانه حملاتی را طراحی می‌کنند از اهداف گروه‌هایی که دارای انگیزه سیاسی هستند، کار بسیار پیچیده‌ای است. (Lynn, 2011)

با وجود این، شناسایی ماهیت و انگیزه‌های واقعی دشمنان در فضای مجازی برای تدوین سیاست‌های کارآمد امنیتی بسیار مهم تلقی می‌شود.

با توجه به این مقدمه کوتاه در این بخش می‌کوشیم به این سؤالات پاسخ دهیم:

ـ منابع مستقیم و غیرمستقیم تهدیدها در فضای سایبر چیست؟

ـ بازیگران اصلی عرصه جنگ سایبر چه کسانی بوده و از چه ماهیتی برخوردارند؟

ـ هدف حملات سایبری چیست؟ آیا هدف حملات سایبری کسب سلطه، برتری سیاسی یا استراتژیکی بوده یا تنها با هدف وارد آوردن ضربات امنیتی بر دولت یا شهروندان طراحی شده است؟

برای پاسخ به این سؤالات می‌توان گفت ماهیت تهدیدها در جنگ‌های سایبری بـه تناسـب بازیگران آن متفاوت است. بنابراین ماهیت تهدیدها در فضای مجازی متناسب با اینکـه ایـن حملات از جانب دولت‌ها، گروه‌های افراط‌گرای ایدئولوژیکی یا سیاسی، مجرمان سازمان‌یافتـه یا گروه‌های کوچک طراحی شده باشد، متفاوت خواهد بود. با وجود این وجه مشترک همـه تهدیدهای سایبر، عدم‌تقارن آنها است. بر همین اساس از جنگ سایبر معمولاً بـا عنـوان جنـگ نامتقارن نیز نام برده می‌شود. در کل می‌توان تهدیدهای سایبری را به موارد ذیل تقسیم کرد:

الف. تهدیدهای مستقیم نظامی در فضای سایبر

تکنولوژی‌های سایبر با دارا بودن عملکردهای بسیار مشخص نظامی مـی‌تواننـد بـه‌طـور مستقیم بر میدان نبرد تأثیرگذار باشند. بخش نظـامی هـر کـشوری بـرای آمـوزش و تجهیـز نیروها، سیستم‌های جنگ‌افزاری، ماهواره‌ها و شبکه‌های ارتباطی یا داده‌پردازی اطلاعـات بـه تکنولوژی‌های سایبری وابسته است. (Meyers, Powers & Faissol, 2009: 10)

در واقع می‌توان گفت فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصـت‌هـای بسیار زیادی را برای نیروهای نظامی هر کشور به‌وجود آورد، به همان میـزان نیـز مـی‌توانـد تهدیدهای بزرگی را برای این بخش ایجاد کند. (Kark, 2010: 2)

بنابراین امروزه سرنوشت جنگ را دیگر تخریب‌ها، انفجارها و عملیات فرسایشی تعیـین نمی‌کنند بلکه از هم گسیختگی ظرفیت‌های فرماندهی و کنترل در فضای مجـازی مـی‌توانـد بسیار برای نتیجه برخوردها تعیین‌کننده باشد. علاوه بر این، امروزه بُعد اطلاعـاتی بـه عنـوان یکی از ابعاد محوری جنگ در همه عملیات‌ها، رزم‌ها و نبردهای آینده دخیـل خواهـد بـود. همچنین در جنگ‌های آینده، کسب برتری سریع در حوزه اطلاعـاتی یکـی از عوامـل مهـم موفقیت خواهد بود. (Rollins & Henning, 2009)

بر همین اساس کشور چین برای مقابله با برتری نظامی ایالات متحده امریکا، مهـم‌تـرین هدف استراتژی‌های نظامی خود را کسب برتری اطلاعـاتی تعریـف کـرده اسـت. در همـین

راستا نیروهای نظامی چین از یک نیروی ماشینی، در حال حرکت به‌سوی یک نیروی اطلاعاتی است. در واقع چین می‌کوشد برای موفقیت در برابر ایالات متحده امریکا اطلاعات را به عنوان یک ابزار مهم به کار برد. در واقع این کشور می‌کوشد فضای مجازی را به عنوان روشی برای کسب برتری در برابر امریکا بدون نیاز به وارد شدن به عرصه نبرد نظامی مورد استفاده قرار دهد. البته چین در همین راستا در تلاش است اصول دفاع فعال را برای آماده‌سازی نیروهایش برای مقابله با تهاجم‌های نظامی در عرصه مجازی، طراحی کند. (Thomas, 2004)

ب. تهدیدهای سایبری غیرمستقیم و غیرنظامی

همان‌گونه که هدف اصلی در جنگ‌های متعارف، از کار انداختن ماشین جنگی دشمن از طریق حمله به ساختار دولت، نهادهای مالی، زیربناهای حیاتی در بخش انرژی و حمل‌ونقل و از میان بردن روحیه و عزم ملی می‌باشد، در جنگ‌های سایبر نیز همین اهداف دنبال می‌شود. (Clarke & Knake, 2010: 3)

یکی از اولین نمونه‌های این نوع از جنگ سایبری در سال ۱۹۸۲ بین اتحاد جماهیر شوروی و امریکا در دوران «ریگان»، زمانی که وی دستور حمله به سیستم خطوط لوله این کشور در سیبری را داد، اتفاق افتاد. با گذشت سال‌ها از آن جنگ، در سال ۲۰۱۰ جدیدترین نمونه این‌گونه از حملات سایبری به‌وسیله حمله کرم «استاکس‌نت[1]» شکل گرفت. این کرم خطرناک که تلاش کرد اطلاعات سیستم‌های کنترل صنعتی را به سرقت برده و آنها را روی اینترنت قرار دهد با اهداف سیاسی و به منظور فشار بر ایران برای توقف طرح غنی‌سازی اورانیوم، نیروگاه‌های اتمی بوشهر و نطنز را مورد هدف قرار داد. (A worm in the centrifuge, 2010)

بنابراین می‌توان به این نکته اشاره کرد که بازیگران جنگ‌های سایبری می‌توانند بدون

1. Stuxnet' worm

نیاز به درگیری‌های نظامی به اهداف استراتژیک و سیاسی خود دست یابند. (McConnell, 2010)

همچنین حمله این کرم خطرناک نشان داد که ماهیت مبهم و نامشخص جنگ‌های سایبر سبب می‌شود که اقدامات مقابله به مثل با مشاجره‌های سیاسی همراه شود و چه‌بسا هزینه‌های بسیار زیادی را برای دولت‌ها به‌وجود آورد. همچنین در جنگ‌های سایبر مرز بین اهداف نظامی و غیرنظامی مبهم است.

ج. تروریسم و افراط‌گرایی

ماهیت نامتقارن، مخفیانه و مجازی فضای سایبر سبب شده است که این فضا، فرصت بسیار مناسبی را برای گروه‌های تروریستی و مجرمان سازمان‌یافته به‌وجود آورد. اگرچه هنوز شواهد محکمی در دست نیست که سازمان‌های تروریستی همانند القاعده بتوانند حملات گسترده نظامی را طراحی نمایند، اما این گروه‌ها از فضای سایبر برای انتشار پیام‌ها، آموزش و سربازگیری، بیشترین استفاده را می‌کنند. فضای اینترنت این امکان را برای گروه‌های تروریستی فراهم می‌کند که تکنیک‌های خود را با یکدیگر به اشتراک گذاشته، پیام‌های خود را اشاعه داده، سربازگیری نموده و به آموزش آنها بپردازند. آنچه موفقیت این گروه‌ها را در فضای سایبر تسریع می‌نماید، ارزان و در دسترس بودن این تکنولوژی‌ها است. (Meyers, Powers, & Faissol, 2009: 25)

د. جاسوسی سایبر

جاسوسی سایبر رایج‌ترین شکل فعالیت در فضای مجازی می‌باشد. جاسوسی سایبر خواه با هدف برملا نمودن اطلاعات مهم حکومتی باشد یا دزدیدن اطلاعات بخش نظامی و بازرگانی، یک عملیات مجازی است که به منظور کسب برتری اطلاعاتی برای دستیابی به موفقیت‌های بزرگتر با صرف کمترین هزینه صورت می‌پذیرد. برای مثال چین تلاش می‌کند که با استفاده از جاسوسی سایبر در ساختارهای مهم سیاسی، اقتصادی و نظامی ایالات متحده امریکا و روسیه نفوذ نماید.

در کل می‌توان گفت، جاسوسی اینترنتی سبب سایش توازن اطلاعاتی بین دولت‌های مختلف می‌شود. البته هدف جاسوسی سایبر تنها دولت‌ها نیستند بلکه شرکت‌های دفاعی، بازرگانی و سازمان‌های غیردولتی بین‌المللی نیز، می‌توانند هدف حملات جاسوسان سایبری قرار گیرند. (Mueller, 2007)

هـ جرایم اقتصادی سایبر

در دنیای معاصر امکان اینکه سازمان‌های اقتصادی هدف حملات سایبر قرار بگیرند، افزایش یافته است. جرایم اقتصادی سایبر یکی از متداول‌ترین اقدامات اقتصادی تهدیدآمیز در عرصه فضای مجازی هستند. جرایم اقتصادی سایبری به اقداماتی اطلاق می‌شود که در فضای مجازی به وسیله سازمان‌های تبهکار به انگیزه کسب سود و منافع مالی صورت می‌گیرد. مهم‌ترین انگیزه این گروه‌ها به دست آوردن پول است. ولی در برخی موارد نیز حملات خود را با هدف آسیب رساندن به اشخاص طراحی می‌کنند. در مورد جرایم اقتصادی سایبر می‌توان گفت این اقدامات مجرمانه که به وسیله سازمان‌های تبهکار با انگیزه مادی طراحی می‌شود، نمی‌تواند در قلمرو جنگ سایبر قرار بگیرد. با وجود این اگر این حملات ادامه یابد با از میان‌بردن توازن مالی یک دولت می‌تواند ضربات جدی را بر ثبات و امنیت یک کشور وارد کند. (همان)

و. جنگ روانی سایبر

مهم‌ترین بعد جنگ‌های سایبر در جهان امروز بعد روانی آن است. عملیات روانی در فضای سایبر اقدامات برنامه‌ریزی‌شده برای انتقال اطلاعات و شاخص‌های منتخب به مخاطبان خارجی است که هدف تأثیرگذاری بر احساسات، انگیزه‌ها، قدرت تفکر و استدلال و نهایتاً تغییر رفتار سازمان‌ها، گروه‌ها و اراده آنها را شامل می‌شود. همچنین ممکن است طراحی عملیات دزدیدن اطلاعات در فضای سایبر با هدف ایجاد تشویش و نگرانی روانی طراحی شود. نمونه این مسئله را می‌توان در مورد کرم استاکس‌نت در ایران نام برد. مهم‌ترین هدف

این کرم خطرناک افزایش ناامنی روانی در میان دولتمردان ایرانی بود. (همان)

چالش‌های امنیتی در 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. چالش‌های امنیتی ایجاد شده در فضای سایبر به تناسب ماهیت طراحان آن از ویژگی‌های خاصی برخوردارند. برای مثال بازیگران دولتی و تروریست‌ها معمولاً با اهداف شبه‌جنگی به طراحی حملات سایبری می‌پردازند. در مقابل هکرها یا گروه‌های تبهکار اقتصادی معمولاً اهداف شبه‌جنگی نداشته و به دنبال کسب منافع مالی یا شخصی هستند. (Glaessner, 2004: 9)

به‌طور کلی می‌توان گفت 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 کرده‌اند. 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 ساخته‌اند. زیرا گسترش تکنولوژی‌های ارتباطی ـ اطلاعاتی فاصله موضوعات داخلی و خارجی را محو کرده و افراد جوامع را با تهدیدهای فراملی پیوند داده است. همچنین این تکنولوژی‌ها با خلق موجودیت‌های بدون ساختار فیزیکی و مجازی و فارغ از محدودیت‌های طبیعی نه تنها حاکمیت ملی دربرخورد با تهدیدهای امنیتی تضعیف نموده بلکه قدرت تأثیرگذاری و عدم‌تعین تهدیدها را نیز افزایش داده است. (Chabinsky, 2010)

اگرچه درگیری در فضای سایبر به علت مبهم بودن منشأ تهدیدها و انگیزه‌های آنها یک

پدیده غیرسیاسی تلقی می‌شود، اما واقعیت امر آن است که حملات سایبر در واقع ادامه سیاست محسوب می‌شوند. یعنی همان‌گونه که جنگ، ادامه فعالیت سیاسی با ابزاری دیگر است؛ حملات سایبری نیز ماهیتی سیاسی دارند. براساس چنین مفهومی تنها آن دسته از حملات سایبری را می‌توان حملات شبه‌جنگی دانست که طراحان آن، اهداف سیاسی را دنبال کنند. (Geers, 2009) یعنی می‌توان گفت ستیز و دشمنی سیاسی در دنیای واقعی با کمک تکنولوژی‌های اطلاعاتی در فضای سایبر دنبال می‌شود. بر همین اساس فضای سایبر یک فضای سیاسی است. بنابراین اگر هدف مهاجمان سایبری دستیابی به منافع مالی یا شخصی از طریق ابزار مجرمانه همانند دزدی، کلاهبرداری یا اخاذی باشد، این اقدامات صرفاً ماهیت مجرمانه دارد اما اگر هدف اصلی مهاجمان سایبر، وارد آوردن آسیب‌های جدی بر نهادهای دولتی، شهروندان یا تخریب و نابودی زیربناها و ساختارهای حیاتی نظامی و غیرنظامی باشد، این اقدامات جزو اقدامات جنگی محسوب می‌شود. (همان)

چالش‌های درگیری در فضای سایبر

محیط سایبر به سرعت در حال تغییر است. این تغییرات و سیال بودن فضای مجازی، چالش بسیار بزرگی را برای کشورهایی نظیر ایالات متحده امریکا به‌وجود آورده است؛ (Meyers, Powers & Faissol, 2009: 11) زیرا این کشور بر فضای سایبری که تفکرات و اندیشه‌های نوین در آن پدید می‌آید و شیوه‌های نوین درگیری طراحی می‌شود، کنترلی ندارد. با گسترش روزافزون دسترسی جهانی به اینترنت و رشد تعداد کاربران نه تنها ترافیک جهانی در فضای سایبر افزایش یافته بلکه بازیگران جدیدی در عرصه امنیت سیاسی، اجتماعی، اقتصادی و فرهنگی جهان، نمود یافته‌اند که به راحتی می‌توانند ماهیت و هویت خود را پشت حکومت‌ها و جنبش‌های اجتماعی مخفی کرده و ضمن طراحی حملات مختلف برای آسیب رساندن به زیرساخت‌های حیاتی یک کشور، زمینه چالش‌های سیاسی و امنیتی را به‌وجود آورند. (همان) از آنجایی که فضای اینترنت بسیار گسترده‌تر از محیط سیاسی کشورها

است؛ دولت‌ها نمی‌توانند بر این فضای مجازی کنترلی داشته باشند. (Goldsmith&Wue, 2008) این مسئله بر شدت چالش‌های ایجاد شده در چنین فضایی می‌افزاید. این مسئله زمانی که با پیچیدگی‌های عمیق فضای مجازی همراه می‌شود، زمینه مناسبی را برای افزایش درگیری و تضاد در این فضا به‌وجود می‌آورد. همین مورد، مفهوم سنتی جنگ را نیز تغییر داده است. در گذشته جنگ مبتنی بر حمله و دفاع بود. اما در حال حاضر به علت پیچیدگی تکنولوژی‌های رایانه‌ای و محیط متغیر و سیال فضای سایبر مفهوم حمله و دفاع تغییر یافته است. به‌گونه‌ای که امروزه دولت‌های مختلف جهان برای تأمین امنیت خود مفهوم دفاع در جنگ‌های سنتی را با مفهوم نرم‌افزاری آن در فضای سایبر تلفیق کرده و در راستای نظامی نمودن این فضا گام برداشته‌اند. در واقع دولت‌های مدرن کنونی می‌کوشند با تلفیق چهار فضای درگیری در زمین، دریا، هوا و فضا با بعد مجازی، درگیری جنگ‌های سایبری را مدیریت نمایند. اما این رویکرد هرچه بیشتر سبب افزایش تنش در فضای مجازی می‌شود. (Rollins & Henning, 2009)

بنابراین می‌توان گفت اگرچه نقش گروه‌های غیردولتی در فضای سایبر افزایش یافته است اما به وضوح می‌توان مشاهده کرد که در زمینه مدیریت جنگ‌ها در فضای سایبر همچنان کنترل نهایی و مسلط با دولت‌های ملی است. علاوه بر این از آنجایی که جنگ چهره‌ای دیگر از سیاست و در واقع دنباله آن به حساب می‌آید، مهم‌ترین راهکار مدیریت جنگ‌های سایبری تدوین یک ساختار سیاسی بین‌المللی به وسیله دولت‌های مدرن ملی خواهد بود. این مسئله نقش دولت‌ها را در فضای مجازی افزایش می‌دهد. بنابراین امروزه شرط اصلی موفقیت مدیریت بحران‌های مجازی، درک فضای سایبر به عنوان یک محیط سیاسی است که نیازمند تدوین ارزش‌ها و هنجارهای بین‌المللی به وسیله دولت‌های جهان می‌باشد. (Kark, 2010:8)

اهمیت فعالیت هماهنگ دولت‌های جهان برای مقابله با بحران‌های جهانی در فضای سایبر به اندازه‌ای است که اکثر کارشناسان، عدم‌موفقیت ایالات متحده امریکا در برخورد با

بحران‌های بسیار پیچیده مجازی را ناشی از یک‌جانبه‌گرایی این کشور در این عرصه می‌دانند. (Rollins & Henning, 2009)

البته همکاری جهانی دولت‌ها برای مدیریت فضای سایبر باید مبتنی بر گفتگو و مذاکره سیاسی باشد. زیرا اتخاذ راهکارهای نظامی تنها منجر به افزایش پراکندگی و تشتت در این فضا می‌شود. مذاکرات سیاسی دولت‌های مدرن ملی در حکم یک سرمایه مهم سیاسی، زمینه تدوین ارزش‌ها و هنجارهای بین‌المللی برای قانونمند کردن این فضا را به‌وجود می‌آورد. در واقع این سرمایه سیاسی از طریق مذاکره سیاستمداران برجسته کشورها که توانمندی تطابق با پیچیدگی‌های فضای سایبر را دارند، شکل می‌گیرد. از آنجایی که در فضای سایبر شناسایی هویت و مکان مهاجم، مقاصد و اهداف آنها سبب ایجاد چالش‌های جدی برای تشخیص به موقع یک تهاجم، واکنش در مقابل آن و ارزیابی دقیق میزان خسارت پس از تهاجم می‌شود لزوم اتخاذ یک چارچوب سیاسی بین‌المللی برای مقابله با چالش‌های فضای سایبر، امروزه یکی از اولویت‌های اصلی امنیت ملی کشورهای جهان محسوب می‌شود. (Lewis, 2008)

البته تأمین امنیت سایبر در بعد داخلی نیز از اهمیت بسیار زیادی برخوردار است. به‌گونه‌ای که امروزه کشورهای اروپایی و ایالات متحده امریکا بیشتر از گذشته به انجام فعالیت‌های سازمان‌یافته در مورد فضای سایبر می‌پردازند. البته در ایالات متحده امریکا هنوز هیچ تفاهم ملی در مورد میزان اهمیت تهدیدهای سایبر حاصل نشده است. به هر حال امروزه دو دسته تفکر در این کشور در مورد تأمین امنیت سایبر شکل گرفته است. گروهی تهدیدهای سایبر را یک مسئله امنیتی تلقی نموده و مسئولیت مقابله با آنها را بر عهده نیروی نظامی می‌دانند. در مقابل گروهی با حضور نظامیان در این عرصه مخالفند و تأمین امنیت مجازی را مسئله‌ای مدنی می‌دانند. با این وجود وزارت دفاع ایالات متحده امریکا نقش تعیین‌کننده‌ای در تعریف منافع این کشور در فضای سایبر ایفا می‌کند. (همان)

دیدگاه بریتانیا نیز درباره جنگ سایبر تا حدی شبیه به امریکا است. این کشور جنگ

سایبر را به صورت اقدامات تأثیرگذار بر سیستم‌های اطلاعاتی دیگران و دفاع از سیستم‌های اطلاعاتی خودی برای کسب حمایت از اهداف ملی تعریف می‌کند. علاوه بر این، بریتانیا از یک چارچوب قانونی برای مدیریت فعالیت‌های اطلاعاتی و مقابله با جرایم رایانه‌ای برخوردار است.

اگرچه این اقدامات می‌تواند در فضای داخلی تا حدی امنیت سایبری را تأمین کند اما برای تأمین امنیت فضای مجازی در بعد جهانی باید همه دولت‌های مدرن غربی و غیرغربی در قالب تعامل‌های سیاسی، یک چارچوب ارزشی و هنجاری را برای تدوین قوانین بین‌المللی برای به نظم درآوردن فضای مجازی شکل دهند. البته ذکر این نکته بسیار مهم، ضروری است که دولت‌های غربی نباید در تدوین ارزش‌ها و هنجارهای بین‌المللی برای قانونمند کردن فضای سایبر نظرهای خود را بر کشورهای غیرغربی تحمیل کنند؛ زیرا چنین اقدامی سبب می‌شود فضای سایبری کشورهای غیرغربی تحت انقیاد قوانین کشورهای غربی قرار گیرد. این مسئله سبب می‌شود، دول غیرغربی قوانینی را برای فضای مجازی خود اجرا کنند که هیچ سنخیتی با محیط داخلی آنها ندارد.

جمهوری اسلامی ایران و جنگ سایبری ایالات متحده امریکا

فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. در فضای سایبر، حضور فراتر از شبکهٔ جهانی وب یا حتی اینترنت است و از انواع ابزارها و امکانات رایانه‌ای و مخابراتی استفاده می‌شود. علاوه بر این با تک تک مخاطبان ارتباط دوسویه و تعاملی برقرار می‌شود و به محتوا بیش از سایر موارد اهمیت داده می‌شود. چرا که فضای سایبر اطلاعات‌محور است. فضای سایبر پدیده جدید دنیای ارتباطات است که علاوه بر مزایای آن، با خود، ابزار گوناگون برای ارتباط تعامل و تبادل فرهنگی و یا

تهاجم و سیطره فرهنگی به همراه آورده و زمینه‌ای مهم برای جنگ نرم است.

تشکیل گروه‌های سیاسی در اینترنت، جاسوسی اینترنتی، تشکیل اجتماعات مجازی، شکل دادن به نافرمانی مدنی، دموکراسی دیجیتالی، افکارسازی از طریق اینترنت، نفوذ و خرابکاری اینترنتی، مبارزه با کنترل خبری حکومت‌ها از طریق اینترنت و کسب اطلاعات از سیستم‌های اجتماعی و سیاسی از طریق اینترنت، مسدود نمودن سایت‌های اینترنتی، فیلترینگ سایت‌ها، رفراندوم اینترنتی، ایجاد گروه‌های سیاسی مجازی، انتقال مستقیم اندیشه‌ها و دیدگاه‌های جریان معاند به داخل، ایجاد گروه‌های فشار و ذی‌نفوذ مجازی، کارکردهای مشروعیتی، ایجاد مطالبات جدید سیاسی، افزایش ضریب نفوذ جریان‌های معاند، افزایش همگرایی گروه‌های داخلی و خارجی همفکر، کاهش نفوذ رسانه‌های ملی و داخلی و گسترش شایعه و خرافات، برخی از راهکارها و تکنیک‌هایی هستند که با استفاده از شبکه‌های اجتماعی برای جنگ نرم علیه کشورمان به‌وسیله ایالات متحده امریکا به‌کار گرفته شده‌اند. (ماه‌پیشانیان، ۱۳۸۹) به‌طورکلی ایالات متحده امریکا می‌کوشد با استفاده از راهکارهای فوق و کاربرد دیپلماسی، تبلیغات، مبارزات روان‌شناسی، انهدام و ترور شخصیتی، سیاسی و تهاجم فرهنگی جنگ نرم جدیدی را ضد کشورمان شکل دهد.

برای بررسی نقش فضای سایبر در جنگ نرم ایالات متحده امریکا بر ضد کشورمان به بررسی مختصر برخی از راهکارهای فوق می‌پردازیم:

ـ تشکیل گروه‌های سیاسی در اینترنت با استفاده از شبکه‌های اجتماعی مجازی:

ایجاد گروه‌های سیاسی اینترنتی که یا به ظاهر وابسته به نهاد یا گروه سیاسی خاصی نیستند یا این موضوع را پنهان کرده‌اند، از روش‌های فعالیت ایالات متحده امریکا بر علیه کشورمان محسوب می‌شود. برخی از روزنت‌های برجسته وابسته به این گروه‌ها، دارای گرایش‌های آشکار ضد نظام بوده و مجموعه‌ای از فعالیت‌های تخریب‌گرایانه علیه سیستم سیاسی ایران را هدایت و رهبری می‌کنند. همچنین بخش اعظم گروهک‌های اپوزیسیون مقیم خارج به دلیل فقدان هرگونه ابزار ارتباطی برای برقراری ارتباط با

مردم ایران، از اینترنت به عنوان مهم‌ترین وسیله ارتباط با داخل ایران استفاده می‌کنند. (ضیایی‌پرور، ۱۳۸۹: ٤)

- **نشت اطلاعات**: استفاده از تکنیک نشت اطلاعات به خصوص اطلاعات محرمانه و سری ایران در فضای سایبر یکی دیگر از روش‌های مقابله معاندان نظام با سیاست‌های رسمی کشورمان است. در آبان ۱۳۸۸، نشت اطلاعات محرمانه نظامی ایران در سایت‌های اینترنتی امریکایی و تلاش برای جذب جاسوسان فارسی زبان از سوی رژیم صهیونیستی از جمله اقدامات انجام شده در این راستا بوده است. در این ماه اعلام شد که برخی اطلاعات سری مربوط به موشک‌های ایران از جمله موشک حوت، روی اینترنت قرار گرفته است. همچنین اعلام شد که سرویس اطلاعاتی «شین بت» اسرائیل، آگهی غیرمعمولی را در روزنامه‌ها چاپ کرده و در جستجوی فارسی‌زبان‌ها است تا آنها را به عنوان جاسوس آموزش دهد. (همان)
- **جاسوسی اینترنتی**: جاسوسی اینترنتی دیگر راهکار ایالات متحده امریکا برای مقابله با کشورمان است. این پدیده عموماً به صورت کسب اطلاعات از طریق برنامه‌هایی معرفی می‌شود که از راه نصب نرم‌افزارها و یا حین گردش افراد در محیط وب وارد کامپیوتر شخصی آنها شده و تا زمانی که کاربر به شبکه جهانی وصل است، اطلاعاتی را که روی هارددیسک او ذخیره شده است برای پایگاه‌های مطلوب خویش می‌فرستند. اما این فقط یکی از انواع جاسوسی الکترونیکی است. جاسوسی اینترنتی همانند جاسوسی سنتی خطرناک و یکی از روش‌های براندازی نرم است. «جرالد نیرو» استاد علم روان‌شناسی در دانشگاه «پرووانس» فرانسه و صاحب کتاب *خطرات اینترنت* در مورد جاسوسی اینترنتی عنوان می‌کند: این شبکه در ماه مه سال ۲۰۰۱ کشف شد و عبارت است از مجموعه شبکه‌هایی که توسط روان‌شناسان اسرائیل اداره می‌شود و مأموریت آنها جذب جوانان کشورهای جهان سوم است. (مستغاثی، ۱۳۹۰) در این شیوه سعی بر آن است که از افراد مخالف با حکومت خود و یا افراد عادی استفاده شود که گرایش‌های

سیاسی ندارند اما قادرند اطلاعات خوبی درباره اماکن و اوضاع ارائه دهند. انتشار پیام استخدام جاسوس اینترنتی به‌وسیله اسرائیل و امریکا برای مقابله با جمهوری اسلامی ایران، از این موارد است. «فارسی صحبت می‌کنی؟ اسرائیل تو را می‌خواهد.» برای مدتی این تیتر روزنامه «هاآرتص» بود. این روزنامه نوشت: «سرویس اطلاعاتی شین‌بت اسرائیل آگهی غیرمعمولی را در روزنامه‌ها چاپ کرده و در جستجوی فارسی زبان‌ها است تا آنها را به عنوان جاسوس آموزش دهد.» به گزارش پرس.تی.وی ـ «بیروت»، روزنامه اسرائیلی «هاآرتص» نوشت: «به نظر می‌رسد که سرویس اطلاعاتی شین‌بت، هدف خود را یافتن افراد فارسی‌زبان برای خنثی‌سازی نفوذ ایران در میان اسرائیلی‌ها قرار داده است.» (همان)

ـ **نافرمانی مدنی الکترونیک**: نافرمانی مدنی الکترونیک که اعتراض‌ها را از خیابان‌ها به فضای مجازی می‌کشاند یکی دیگر از روش‌های ایالات متحده امریکا برای مقابله با ایران است. تظاهرات مجازی، نفوذ به به سایت‌های پربیننده و درج تصاویر، خبرها و مطالب سیاسی علیه حکومت و استفاده از بمب‌های جستجوگر از مهم‌ترین روش‌های نافرمانی مدنی الکترونیکی است که برای اولین بار توسط گروهی با نام «گروه هنر انتقادی» در سال ۱۹۹٤ و در کتابی تحت عنوان *اختلال الکترونیک* مطرح شد. بخشی از اهداف نافرمانی مدنی الکترونیک، مبارزه اطلاعاتی مردمی و یا مبارزه اطلاعاتی از پایین است که در این مبارزه نه حکومت بلکه مردم و به‌طور مستقیم به شکل دادن جریان اطلاعات در جهت مبارزه با حاکمیت و یا بیان اعتراض خود نسبت به معضلات اجتماعی و سیاسی می‌پردازند. این مبارزه صرفاً مبارزه براساس حروف در فضای مجازی است اما قدمی مؤثر و اصلی در جهت شکل گرفتن یک جریان اجتماعی و فشار بر هیئت حاکمه است. (ماه‌پیشانیان، ۱۳۸۹)

ـ **دموکراسی دیجیتال**: یکی دیگر از راهکارهای ایالات متحده امریکا برای براندازی نرم، ترویج دموکراسی با استفاده از ابزارهای نوین تکنولوژی‌های دیجیتالی است که

دموکراسی دیجیتال نامیده می‌شود. راه‌اندازی چندین مؤسسه تحقیقاتی و رسانه‌ای همچون «خانه آزادی، واشنگتن پریزم»، «بنیاد دموکراسی برای ایران» و حمایت از برخی وب‌سایت‌ها و روزنت‌های موجود اینترنتی و سایر رسانه‌های ماهواره‌ای نیز در دستور کار امریکا قرار دارد. «مرکز کمک بین‌المللی رسانه‌ای» موسوم به «سیما» Center For International Media Assistance (CIMA) از جمله سازمان‌های غیرانتفاعی امریکایی است که هدف آن به ظاهر ترویج دموکراسی در جهان از طریق حمایت از رسانه‌های همسو است. این مرکز در زمینه ایجاد شبکه‌های رسانه‌ای و هدایت پژوهش‌هایی که در این مورد انجام می‌شود و همچنین برگزاری نشست‌هایی با موضوع ضرورت نقش رسانه‌های آزاد و مستقل در برقراری دموکراسی و براندازی نرم در جهان فعالیت می‌کند. منابع مالی این مرکز از سوی دولت امریکا و براساس قانون مصوب سال ۱۹۸۳ تأمین می‌شود. (عبدالله‌خانی؛ کاردان، ۱۳۹۰) به موجب این قانون که در زمان ریاست‌جمهوری «رونالد ریگان» در کنگره امریکا تصویب شد، این کشور سالانه بودجه‌ای را برای ترویج دموکراسی در جهان اختصاص می‌دهد. در این میان وضعیت رسانه‌های ایران از جمله موضوعاتی است که مورد توجه مرکز سیما است. کارشناسان برایند فعالیت‌های چنین مراکزی را قانونی جلوه دادن، منطقی و دموکراتیک القا کردن فعالیت‌های رسانه‌ای علیه حکومت‌های ضدامریکا و صهیونیسم ارزیابی می‌کنند. ایالات متحده امریکا با استفاده از شبکه‌های اجتماعی و روش‌های مذکور به ساماندهی اغتشاشات و نشر و گسترش شایعات برای مقابله با جمهوری اسلامی ایران می‌پردازد.

ـ **جنگ فیلتری**: یکی دیگر از شیوه‌های جنگ نرم امریکا با استفاده از شبکه‌های مجازی، جنگ فیلتری است. با افزایش دامنه جنگ فیلترها، برخی سایت‌های اینترنتی روش‌های جدید برای عبور از سد فیلترینگ را به کاربران آموزش می‌دهند. در یکی از این روش‌ها آمده است: فیلترشکن دائمی و با سرعت فوق‌العاده داشته باشید. تنها چیزی که برای این فیلترشکن احتیاج دارید یک مقدار اندک، هاست یا همان فضای اینترنتی است.

کافی است فایل خاصی را دانلود کنید. بعد آن را از حالت زیپ درآورده و محتویاتش را داخل هاست خودتان بریزید. فیلترشکن‌تان آماده است. (ضیایی‌پرور، ۱۳۸۹: ۱۰)

ـ تروریسم روانی، انتشار مطالبات قومی منطقه‌ای و افزایش تحریک‌پذیری قومیت‌ها: این روش، دیگر راهکار ایالات متحده امریکا در جنگ نرم شبکه‌ای با ایران است. خاصیت تأسیس سایت‌های قومی، راه‌اندازی وبلاگ‌های منطقه‌ای و انتشار برخی مطالب تحریک‌آمیز در سایت‌های اینترنتی، قابلیت این رسانه را برای دامن زدن به مباحث مناقشه برانگیز قومی بالا برده است. بر همین اساس ایالات متحده امریکا می‌کوشد با کاربرد شبکه‌های اجتماعی مجازی به مطالبات و تحرکات قومی دامن بزند. بر همین اساس در تلاش است با استفاده از سلاح‌هایی همچون تبلیغات، شایعه‌سازی، دروغ‌پراکنی و تشویش اذهان عمومی و هدف قرار دادن نظام باورها، شالوده‌های فکری و روح و روان مردم با تلفیق هوشمندانه و هدفمند مسائل قومی با اهداف سیاسی و ایدئولوژیک خود به جنگ نرم با ایران بپردازد. بدین ترتیب ایالات متحده امریکا با دامن زدن به مطالبات قومی از طریق شبکه‌های اجتماعی مجازی سعی در ایجاد ناامنی روانی در جامعه داشته و برآنست مسئله قومیت‌های ایرانی را به ابزار فریب و تنش ذهنی برای مردم ایران تبدیل کند. این اقدام ایالات متحده امریکا می‌تواند به گروه‌های معاندی همچون جندالشیطان کمک نماید که با کاربرد شبکه‌های مجازی در پی جلب افکار عمومی و جذب نیروها و کادر سیاسی ـ رزمی جدید، مشروعیت‌سازی، مظلوم‌نمایی و ارائه تصویر قوی، قدرتمند و اسطوره‌ای اقدام کنند و با تشدید احساس ناامنی در بین شهروندان همراه با کاهش آستانه تحمل و بردباری مردم، هراس‌افکنی و وحشت‌زایی، ذهنیت‌سازی و القای مهارناپذیر بودن حملات برآمده و بدین ترتیب با کشاندن دولت ایران به بن‌بست امنیتی به باج‌گیری سیاسی و ضربه زدن به نظام سیاسی کشورمان بپردازند. بنابراین همان‌طور که اشاره شد ایالات متحده امریکا به کمک کاربرد شبکه‌های اجتماعی مجازی و با راهبرد بحران‌زایی در

درون و فشار از بیرون به جنگ نرم با کشورمان اقدام می‌کند. (ماه‌پیشانیان، ۱۳۸۸)

ـ **فرقه‌گرایی از طریق اینترنت و حمایت از اقلیت‌های مذهبی**: یکی دیگر از روش‌هایی است که امریکا برای پیشبرد اهداف خود در ایران از آن سود می‌جوید. برای مثال می‌توان به حمایت ایالات متحده امریکا از شبکه‌هایی همانند «انجمن نژاد پرستان بلک متال» (ترویج نژادپرستان ایرانی)، «جنبش شیطان‌پرستان ایرانی»، «جنبش آریانیسم» و .... اشاره کرد.

جمع‌بندی

در دهه‌های اخیر به واسطه رشد و گسترش روزافزون تکنولوژی‌های اطلاعاتی ماهیت و روش‌های جنگ تغییر یافته است. در شیوه‌های نوین درگیری برخلاف روش‌های سنتی تنها دولت ـ ملت‌ها با روش‌ها و ابزار سخت‌افزاری با یکدیگر درگیر نیستند بلکه به واسطه تغییر ماهیت تهدیدها، روش‌های درگیری نیز تغییر چشمگیری یافته است. در شیوه‌های نوین جنگ، ابعاد درگیری به میدان نبرد محدود نمی‌باشد، بلکه به علت ترکیب عملیات نظامی با اقدامات خصمانه در عرصه اقتصادی، نظامی، سیاسی و دیپلماتیک، ابعاد آن به خارج ازمحیط درگیری نیز سرایت پیدا می‌کند. در شیوه‌های نوین درگیری تنها هدف که دستیابی به پیروزی است، مهم تلقی می‌شود. بنابراین نیروهای متخاصم ممکن است برای رسیدن به چنین هدفی درگیری را با هر روش و تاکتیکی به قلب جامعه، فرهنگ، آگاهی و وجدان عمومی گسترش دهند. بنابراین می‌توان گفت امروزه به واسطه رشد تکنولوژی‌های سایبری، متخاصمان می‌توانند به آسانی دامنه درگیری را تا ذهن و روان مردم بکشانند و با استفاده از کوچکترین و کم هزینه‌ترین ابزار گسترش دهند.

ایالات متحده امریکا با استفاده از قابلیت‌های فضای سایبر در زمینه تولید آسان و ارزان مطلب همراه با استفاده از جاذبه‌های رنگین تلاش دارد به هویت‌های اجتماعی مخالف نظام جمهوری اسلامی ایران در فضای سایبر شکل دهد و با فراهم کردن امکان زیست مستعار

جنبش‌های‌اجتماعی مخالف در این فضا به آنها این توانمندی را بدهد که با سوء استفاده از بحران‌های اجتماعی، سیاسی و اقتصادی موجود در جامعه به هویت جمعی مجازی مخالف نظام شکل دهد و بدین ترتیب و با متقاعد نمودن پیروان خود، آنها را متناسب با اهداف مورد نظر خود در عرصه جنگ نرم، بسیج کند. این هویت‌های مجازی به علت عدم توانایی در زمینه نهادسازی سیاسی در جریان اعتراضات، فضای سیاسی را از فرایند عقلانی خارج و با گسترش فضای آشوب و شایعه و فراهم نمودن زمینه لازم برای شکل‌گیری جهل عمومی، مأموریت خود را در عرصه جنگ نرم، به انجام می‌رسانند.

بر همین اساس می‌توان گفت امروزه افزایش توانمندی ملی برای مقابله با ابهام، پیچیدگی و پویایی تهدیدهای امنیتی مهم‌ترین راهکار برای حفظ منافع ملی کشورمان در فضای سایبر است. لذا استراتژی امنیت ملی کشورمان پل ارتباطی بین اهداف، روش‌ها و ابزارهای منافع ملی خواهد بود. با توجه به چنین تعریفی می‌توان گفت یک استراتژی موفق برای تأمین امنیت سایبر، نیازمند تعریف اهداف، روش‌ها و وسایل جدید در تلازم با محیط سیاسی است.

علاوه بر این از آنجایی که جنگ سایبر دارای ابعاد استراتژیک می‌باشد برای موفقیت استراتژی دفاع سایبری باید اهداف، وسایل و روش‌های آن به وسیله کارشناسان دفاعی و نظامی کشورمان شناخته شود. جنگ سایبر مجموعه‌ای از عقاید، کنش‌ها و واکنش‌هایی است که بدون قرار گرفتن در یک چارچوب مشخص سیاسی، نظامی، اقتصادی و فرهنگی عمل می‌کنند. البته این مسئله به مفهوم بی‌قاعدگی فضای سایبر نمی‌باشد بلکه شبکه‌های اجتماعی نوین همانند فیس‌بوک از قوانین خاص خود برخوردار هستند. همچنین عضویت افراد در این شبکه‌ها سبب افزایش سرمایه اجتماعی و کاهش اختلافات می‌شود. با این وجود قانونمند شدن فضای سایبر، نیازمند تدوین ارزش‌ها و هنجارهای جهانی با مشارکت سیاسی همه کارشناسان است.

نکته کلیدی برای موفقیت مدیریت بحران در فضای سایبر، شناخت انگیزه انجام حملات سایبری است. یعنی جمهوری اسلامی ایران هنگام تدوین ارزش‌ها و هنجارها برای قانونمند

نمودن فضای سایبر باید بین حملات سایبری به عنوان یک عمل مجرمانه یا یک عمل با مقاصد سیاسی تفاوت قائل شود. البته این تمییز قائل شدن، از پیچیدگی بسیار زیادی برخوردار می‌باشد. زیرا دولت نمی‌تواند به راحتی بین چالش‌های ناشی از جنگ، افراط‌گرایی، جرایم و آسیب‌های سایبری تمایز قائل شود. زیرا همه این موارد، تاکتیک‌ها، تکنیک‌ها و روش‌های مشابه به کار می‌برند. با این حال دولت جمهوری اسلامی ایران باید بتواند به شناخت صحیحی از انگیزه‌ها، ماهیت و اهداف حمله‌کنندگان سایبری دست یابد تا بتواند به واکنش مناسب در برابر آنها بپردازد.

همان‌گونه که اشاره شد؛ جنگ سایبر، شیوه نوین درگیری دولت‌ها در فضای سایبر است که با شیوه سنتی جنگ تفاوت بسیار زیادی دارد. بر همین اساس در کنار تدوین ارزش‌ها برای قانونمند نمودن آن، کشورمان باید قدرت سایبری خود را نیز افزایش دهد. افزایش قدرت سایبری رمز موفقیت سیاست‌های هماهنگ دولت برای مدیریت فضای مجازی می‌باشد.

در حال حاضر به علت فقدان قوانین مدون برای مدیریت فضای مجازی، این فضا برای گروه‌های مختلف دولتی و غیردولتی به منظور دستیابی به اهداف سیاسی، اقتصادی، فرهنگی، اجتماعی و حتی نظامی جذابیت خاصی یافته است. بنابراین از آنجایی که جنگ سایبر ادامه سیاست با ابزار دیجیتال است، تنها با اتخاذ سیاست‌های هوشمندانه می‌توان آن را کنترل کرد. در همین راستا می‌توان گفت این دولت است که می‌تواند با اتخاذ چارچوب‌های سیاسی فضای سایبر را مدیریت کند.

درک کردن جنگ سایبر به عنوان یک مجموعه مرتبط به هم، افزایش توانمندی‌های تکنولوژیکی به منظور افزایش قدرت سایبر و پی‌بردن دولت به محدودیت‌های خود برای مقابله یک‌جانبه با چالش‌های جنگ سایبر، سه گام بسیار مهم در موفقیت مدیریت فضای مجازی محسوب می‌شود. بنابراین اگر جنگ سایبر به عنوان یک پدیده سیاسی ـ استراتژیک درک شود، بسیاری از مشکلات برای مدیریت کردن فضای سایبر حل می‌شود. شناسایی دقیق

اهداف حمله‌کنندگان، همکاری سیاسی بین‌دولتی، قاعده‌مند نمودن و گسترش ارتباطات استراتژیک در بعد داخلی و بین‌المللی، چهار راهکاری است که در این زمینه بسیار مهم می‌باشد.

در یک جمع‌بندی نهایی می‌توان گفت رویکردهای دولت‌محور و سیاسی ـ نظامی صرف، برای مقابله با چالش‌های جنگ سایبر کافی نیست. زیرا جنگ سایبر در یک محیط بسیار پیچیده، سیستماتیک، متغیر و سیاسی رخ می‌دهد. بنابراین مدیریت آن نیازمند تدوین یک استراتژی امنیت ملی است. بر همین اساس ارزش‌ها و هنجارهای مشترک سیاسی می‌توانند آن را قانونمند کنند. زیرا نظامی کردن فضای سایبر تنها سبب افزایش تشتت در آن شده و احتمال اختلاف و درگیری را شدت می‌بخشد. در همین زمینه دولت جمهوری اسلامی ایران باید بکوشد قدرت سایبری خود را افزایش دهد. زیرا امروزه برای پیروزی در پنجمین عرصه نبرد، تنها تکنولوژی به همراه ارزش‌ها و هنجارهای اخلاقی ـ سیاسی می‌تواند حرف نهایی را بزند.

در پایان می‌توان راهکارهای ذیل را برای مقابله با تهدیدها در فضای سایبر پیشنهاد کرد:

ـ آموزش: تهیه ابزار مناسب برای تمرین و توسعه توانمندی‌های نیروهای انسانی برای مقابله با تهدیدهای سایبر؛

ـ تجهیزات: تهیه سیستم‌ها، سلاح‌ها و خط‌مشی‌ها برای مجهز کردن اشخاص، گروه‌ها یا سازمان‌ها در جنگ سایبر؛

ـ توانمندسازی کارکنان: توسعه توانمندی‌های کارکنان بخش‌های مختلف و مهم سازمان‌های اطلاعاتی و امنیتی برای شناسایی تهدیدها و مقابله با آنها در فضای سایبر؛

ـ اطلاعات: توسعه توانمندی‌های برای جمع‌آوری، شناسایی و تحلیل اطلاعات؛

ـ دکترین و مفاهیم: تدوین دکترین‌های اطلاعاتی و امنیتی برای حفاظت از زیرساخت‌های اطلاعاتی و حیاتی و حفظ مفاهیم مهمی که در آینده برای امنیت سایبر دارای اهمیت است؛

ـ حفظ روابط سازمانی و غیرسازمانی بین بخش‌های مهم اطلاعاتی؛
ـ حفظ، توسعه و مدیریت اطلاعات برای تأمین امنیت زیرساخت‌های حیاتی؛
ـ اقدامات لجستیکی: افزایش دانش و توانمندی طراحی و اجـرای عملیـات اطلاعـاتی و حفظ برتری نیروها.

فهرست منابع

ـ ضیایی پرور، حمید، (۱۳۸۹)، ***جنگ سایبری بعد از انتخابات***، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

ـ عبدالله خانی، علی، کاردان، عباس، (۱۳۹۰)، ***رویکردها و طراح‌های امریکایی درباره ایران***، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

ـ ماه‌پیشانیان، مهسا، (۱۳۸۸)، «**تبیین منازعات قومی براساس تئوری‌های مداخله: نگاهی به تهدیدات نرم ایالات متحده امریکا برای جمهوری اسلامی ایران**»، فصلنامه علمی ـ تخصصی عملیات روانی، سال ششم، شماره ۲٤، زمستان.

ـ ماه‌پیشانیان، مهسا، (۱۳۸۹)، «**بررسی ابعاد اجتماعی ـ فرهنگی جنگ نرم امریکا علیه جمهوری اسلامی ایران**»، فصلنامه علمی ـ تخصصی عملیات روانی، سال هفتم، شماره ۲٦، تابستان.

ـ مستغاثی، سعید، (۱۳۸۹)، به بهانه تقدیر از فیلم «شبکه اجتماعی» در جشنواره‌های غربی: تارهای یک شبکه صهیونیستی: ۸ اردیبهشت، روزنامه کیهان: http://www.kayhannews.ir/900208/9.htm

- **"A worm in the centrifuge".** (2010, October 02). Retrieved from The Economist: <http://www.economist.com/node/17147818>

- Billo, C., & Chang, W. (2004, December). "**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>
- Carr, C. (2003). ***The Lessons of Terror: A History of Warfare Against Civilians***. New York: Random House Trade Paperback.
- Chabinsky, S. R. (2010, March 23). "**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>
- Clarke, R., & Knake, R. (2010). ***Cyber War***. New York: Ecco.
- Clarke, R., & Knake, R. (2010). ***Cyberwar: The Next Threat to National Security and What to Do About it***. New York: HarperCollins.
- Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. "**Information Security Journal: A Global Perspective**", 18 (1).
- Glaessner, T. C. (2004). **Electronic Safety and Soundness: Securing Finance in a New Age**. World Bank Working Paper (26).
- Goldsmith, J., & Wu, T. (2008). ***Who Controls the Internet?***. oxford: oxford University Press.
- Kark, K. (2010, August 13). "**The New Threat Landscape: Proceed With Caution**". Retrieved from Forrester Research, Inc.: <www.federalnewsradio.com/docs/The_New_Threat_Landscape.pdf>
- Krebs, B. (2009, April 15). "**organized Crime Behind Data Breaches**". Retrieved from The Washington Post: < http://www.washingtonpost.com /wp-dyn/content/article/2009/04/15/AR2009041501196_3.html?sid= ST2009041501334>
- Lee, A. (2011, June 13). "**CIA Chief Leon Panetta: Cyberattack Could Be Next Pearl Harbor** ". Retrieved from Huffington Post: <http://www. huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n _875889.html>
- Lewis, J. A. (2008, December 8). "**Securing Cyberspace for the 44th Presidency**". Retrieved from Center for Strategic and International Studies (CSIS): <http://www.csis.org/publication/securing-cyberspace-44th-presidency>
- Lynn, W. J. (2011, February 15). "**Remarks on Cyber at the RSA Conference**". Retrieved from U.S. Department of Defense: <http:// www.defense.gov/speeches/speech.aspx?speechid=1535>
- McCarthy, D. (2011). "**open Networks and the open Door: American Foreign Policy and the Narration of the Internet**". Foreign Policy

- Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009, October 08). "**Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches**". Retrieved from Lawrence Livermore National Laboratory (LLNL): <http://www.osti.gov/bridge/servlets/purl/967712-BNpjlx/967712.pdf>
- Mueller, R. S. (2007, January 11). ***Testimony Before the Senate Select Committee on Intelligence***. Retrieved from The Investigative Project on Terrorism: <http://www.investigativeproject.org/documents/testimony/71.pdf>
- Rattray, G. J. (2001). ***Strategic Warfare in Cyberspace***. Cambridge, MA: MIT Press.
- Rollins, J., & Henning, A. C. (2009, March 10). "**Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations**". Retrieved from Congressional Research Service : <http://www.whitehouse.gov/files/documents/cyber/Congressional% 20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities %20and%20Policy%20Considerations%20(March%202009).pdf>
- Schaap, A. J. (2009). ***Cyber warfare operations: development and use under international law***. Air Force Law Review.
- Shachtman, N. (2011, July 15). "**Pentagon makes love, not cyber war**". Retrieved from CNN Tech: <http://articles.cnn.com/2011-07-15/tech /pentagon.cyber.war.wired_1_cyber-war-pentagon-strategy-dod?_s=PM: TECH>
- Thomas, T. L. (2004). ***Dragon bytes: Chinese information-war theory and practice from 1995-2003***. Leavenworth County, Kansas: Foreign Military Studies Office.
Analysis, 7 (1).