



نقش رسانه‌های اینترنت در ناهنجاری‌های اجتماعی در فضای سایبری در میدان جنگ نرم

مهدی عباسی *

تورج هاشمی **

تاریخ دریافت مقاله: ۸۹/۱۰/۱۱

تاریخ تأیید مقاله: ۸۹/۱۲/۱۵

چکیده:

مفاهیم قدرت و جنگ نرم، پس از یک دوره انباشت ادبیات آن در طول جنگ سرد در واپسین سال‌های قرن بیستم و آغازین روزهای هزاره جدید به پارادایم حوزه‌های سیاسی - امنیتی - فرهنگی تبدیل شد. مفهوم قدرت از تصلب سخت‌افزاری به کنش‌های نرم‌افزار گرایانه گرایش یافت و آرایش‌های سیاسی پیوسته مقالات فرهنگ و اندیشه گردیدند. در این میان اینترنت را باید بزرگترین سامانه‌ای دانست که تاکنون به دست انسان طراحی، مهندسی و اجرا شده است. این سامانه شبکه‌ای عظیم از میلیون‌ها رایانه است که کاربران مختلف و اهداف متعددی دارد؛ ولی در نهایت بصورت یک شبکه جهان‌شمول، واحد و در مقیاس جهانی به هم متصل است و این کاربر رسانه‌ای و نقش آن در تهییج جنبش‌های اجتماعی که به سرعت مرزهای کشورها را در می‌نوردد و موجب ناهنجاری‌های اجتماعی می‌شود، قابل چشم‌پوشی نیست. بنابراین امروزه اهمیت و جایگاه اینترنت را در فضای سایبری برای کشورها دو چندان کرده است.

در این مقاله با ارائه تعریفی از مفهوم جنگ نرم، آسیب‌های اجتماعی - سیاسی - فرهنگی اینترنت در فضای مجازی ارائه و راهکارهای دفاع در برابر سایبر تروریسم مورد بررسی قرار می‌گیرد.

واژگان کلیدی: جنگ نرم، فضای مجازی، اینترنت و سایبر تروریسم.

مقدمه

پژوهش، ابتدا به معرفی چیستی جنگ نرم پرداخته، جهت و جایگاه اینترنت بعنوان بزرگترین سامانه در عصر مجازی و ابعاد آسیب‌های آن تا چه حدی می‌تواند برای کشورها تأثیرگذار باشد، پرداخته می‌شود.

پیشینه تحقیق

در زمینه جایگاه فضای سایبری در جنگ نرم، پژوهش‌های بسیاری انجام گرفته که اینجا به برخی از مهمترین آنها اشاره می‌شود. حجت‌الله مرادی در پژوهشی با عنوان: «زبان، ابزار قدرت نرم در ارتباطات نامتقارن اینترنتی» کاربرد اینترنت با زبان انگلیسی که اجزای جدایی‌ناپذیر یکدیگر بوده و میلیون‌ها کاربر اینترنتی ناگزیرند برای استفاده از اینترنت با این زبان آشنا شوند و این برای کشورهای غربی فرصتی را فراهم می‌کند که در فضای جنگ نرم به اهداف خودشان برسند، پرداخته است.

مهسا ماه پیشانیان در پژوهشی با عنوان: «گفتمان جنگ مجازی و رسانه‌های گروهی» معتقد است: رسانه‌های گروهی می‌توانند شرایط جنگ را از طریق تبدیل و تخفیف مرگ در طی جنگ‌ها، شبیه‌سازی، مسافت‌سازی، فضیلت‌مند جلوه دادن جنگ، دگرگون‌سازی طبیعت جنگ، راه یافتن جنگ مجازی به همه صفحه‌های نمایشی، تلویزیون، رایانه، سینما تغییر دهند که اینترنت و تبلیغات نیز در تغییر شرایط جنگی و مجازی‌سازی مؤثر بوده‌اند.

مرتضی عزیزی در مقاله‌ای بنام «سایبر تروریسم یا تروریسم اینترنتی» با ارائه تعریفی از تروریسم، نوع و جذابیت آن آموزش‌های دفاعی - سازوکارهای حقوقی را برای شهروندان و حتی برخی از مدیران در خنثی‌سازی فرهنگ غربی، مقوله جنگ نرم را لازم می‌داند.

روش تحقیق

برای شناخت نقش رسانه‌های اینترنت در فضای جنگ نرم و در پاسخ به این سؤال که اینترنت به عنوان کاربری که میلیون‌ها انسان از آن استفاده می‌کند، چه نقشی می‌تواند در جنگ نرم ایفا کند؟ با مطالعه مقالات و کتاب‌ها راجع به فضای مجازی و جنگ نرم و مشاوره با اساتید برجسته و با تعمق و اندیشه راجع به آنها،

ظهور جامعه شبکه‌ای که از ویژگی‌های نظام سرمایه‌داری متکی به اطلاعات است نتایج و پیامدهایی از جمله فرهنگ واقعیت مجازی، سیاست بر بال رسانه، زمان بی‌زمان و جنگ مجازی را همزمان با انقلاب اطلاعاتی همراه خود آورده است و واسطه‌های الکترونیک، فرهنگ عصر اطلاعات را در چارچوب انتقال نمادها شکل می‌دهند. این واسطه‌های متنوع با مخاطبان گوناگونی سروکار دارند و مجموعه‌هایی غنی از نظر محتوای نمادین و در چارچوب متون الکترونیک در اختیارشان قرار می‌دهند. به این ترتیب این فضای مجازی، شامل اطلاعات زیاد و متنوع، بخشی از واقعیت اجتماعی عصر جدید است و در این فضای فرهنگی متکی به واقعیت مجازی، بازیگران سیاسی به‌منظور حضور در صحنه و تأثیرگذاری بر روند تحولات، ناگزیر از رسانه‌های حامل نمادهای الکترونیک اعم از تلویزیون و رادیو و از همه مهمتر اینترنت بیشترین استفاده را می‌برند. پیامی که در عرصه سیاست از طریق رسانه‌های الکترونیک منتقل می‌شود به اقتضای ماهیت رسانه و انباشت اطلاعات و داده‌ها صورتی ساده به خود می‌گیرد. افشاگری‌ها، بازگویی رسوایی‌های اخلاقی و مالی، برجسته کردن فقدان مشروعیت سیاسی در رقیب از مؤثرترین ابزار فعالیت سیاسی در این عرصه هستند.

بر این اساس در فضای سایبر مقوله‌ای بنام جنگ نرم است که به این صورت تعریف می‌شود: «استفاده طراحی شده است از تبلیغات و فعالیت‌ها به جای جنگ فیزیکی و انتقال عقاید و اطلاعاتی که برای تأثیرگذاری عقاید، نگرش‌ها، احساسات و رفتار گروه‌های خارجی در نظر گرفته شده‌اند، به شکلی که از تحقیق اهداف ملی حمایت کند.»

در عصر سایبر، جهان جدید به شبکه نیرومندی تبدیل شده است که بافت اصلی و تار و پود آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. در درون این شبکه، به‌جز گروهی از نخبگان دیگران کنترل خود را بر زندگی خویش و محیط پیرامون از دست داده‌اند یا به‌سرعت در حال از دست دادن آنند. به‌خصوص با ورود و گسترش پدیده اینترنت به عرصه تعاملات اجتماعی، سیاسی، اقتصادی بشر و ارتباط آن با مقوله جنگ نرم رژیم‌های سخت را به تکاپو انداخته است، در این روش

تنظیم اولویت‌های طرف مقابل، به‌وسیله ابزارهایی مانند فرهنگ، انتقال ارزش‌ها و نهادهای اجتماعی و از طریق دیپلماسی عمومی اعمال می‌شود (احمدزاده کرمانی و اسماعیلی، ۱۳۸۷: ۶۸).

قدرت نرم، برخلاف «قدرت سخت» که دارای ساختارهای با منطق سلسله‌مراتبی و از سمت بالا به پایین است، در ساختاری دایره‌ای و فاقد اضلاع تعریف می‌شود که در آن، برخلاف مدل سلسله‌مراتبی - که امکان دیالکتیک تمام اجزاء در آن واحد میسر نیست - منطق دیالکتیک در آن بازتولید می‌گردد که در نمودار زیر نشان داده می‌شود:

اما دومین مفهوم در کنار مفهوم قدرت نرم، مفهوم تهدید نرم است. تهدید را می‌توان تحولاتی دانست که موجب دگرگونی در هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام سیاسی می‌شود. تهدید نرم، نوعی زمینه مسلط در ابعاد سه‌گانه حکومت، اقتصاد و فرهنگ است که از طریق استحاله الگوهای رفتاری در این حوزه‌ها و جایگزینی الگوهای نظام سلطه، محقق می‌شود (احمدزاده کرمانی، ۱۳۸۸: ۱۴۳).

برخلاف تهدید سخت که متکی بر روش‌های فیزیکی، عینی، سخت‌افزارانه و همراه با اعمال و رفتارهای خشونت‌آمیز، براندازی آشکار و با استفاده از شیوه اجبار و اشغال سرزمینی است، تهدید نرم، بدون مزاحمه و لشگرکشی فیزیکی انجام می‌گیرد و محصول پراورش ذهنی نخبگان این حوزه وسایل اجتماعی، فرهنگی و سیاسی است. در حالی که حوزه هر تهدید سخت، امنیتی و نظامی است (نائینی، ۱۳۸۶).

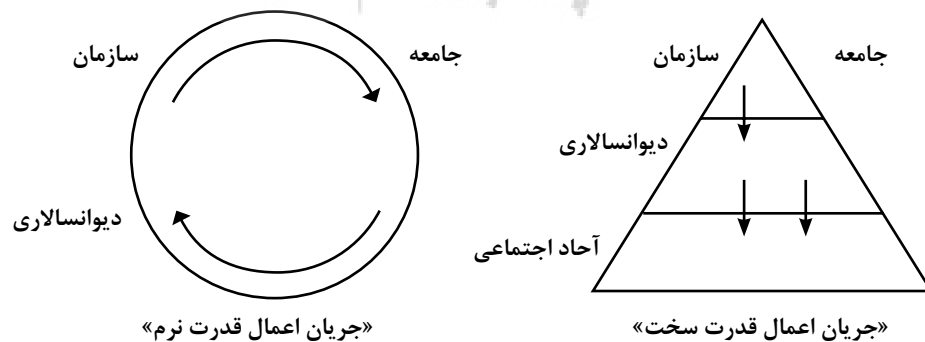
بر این اساس در فضای تهدیدها و قدرت نرم، جنگ نرم در حقیقت شامل هرگونه اقدام نرم‌افزارانه اعم از روانی - تبلیغاتی،

برخی از آسیب‌هایی که کاربر اینترنت می‌تواند در ایجاد ناامنی‌های اجتماعی نقشی داشته باشد، مورد بررسی قرار می‌گیرد.

پس از تجزیه و تحلیل، ویژگی‌های اینترنت به‌عنوان چالش‌های فراروی جنگ نرم برای غربی‌ها و برای دستیابی به سازوکارهایی در جهت دفع فضای سایبر تروریسم، راهکارهایی ارائه شده و مورد بررسی قرار می‌گیرد.

چیستی جنگ نرم

برای فهم دقیق‌تر «اصطلاح جنگ نرم» باید دو اصطلاح دیگر را بررسی کنیم که شامل «قدرت نرم» و «تهدید نرم» هستند. قدرت نرم به‌معنای توانایی رسیدن به اهداف مورد نظر از طریق جلب دیگران به جای استفاده از زور دانسته شده است. قدرت نرم، محصول و برآیند تصویرسازی مثبت، ارائه چهره موجه از خود، کسب اعتبار در افکار عمومی داخلی، خارجی و قدرت تأثیرگذاری غیرمستقیم توأم با رضایت بر دیگران دانسته شده است (نای، ۱۳۸۲). از چشم‌انداز ارتباطات بین‌المللی می‌توان قدرت را در مرحله روابط بین‌المللی به سه دسته کلی تقسیم کرد: قدرت سخت یا همان قدرت نظامی، قدرت اقتصادی و قدرت نرم که هر یک از این سه نوع قدرت برای مقاصد خاص، با نمودارهای رفتاری متفاوت و در سیاست‌های مختلفی به‌وسیله حکومت‌ها اعمال می‌شوند. قدرت نظامی به قصد اجبار و بازدارندگی طرف مقابل و از طریق دیپلماسی قهرآمیز اعمال می‌گردد. قدرت اقتصادی به قصد ایجاد نوعی برانگیختن کشورهای خاص و از طریق تشویق یا تحریم اقتصادی یا تضييع و کمک‌های مالی اعمال می‌شود. اما قدرت نرم با نیت ایجاد جذابیت برای خود یا



نمودار ۱. جریان اعمال قدرت (افتخاری، ۱۳۸۷: ۱۸)

گروه‌های اجتماعی را تحت تأثیر قرار می‌دهد. به عبارت دیگر؛ هرگاه فرایندهای جنگ نرم ظهور یابد، نشانه‌هایی از قدرت‌سازی حکومتی با چالش روبه‌رو می‌شود. در این ارتباط، شاهد عدم تقارن در فضای جنگ نرم هستیم.

تصاویر در فضای ارتباطی جدید می‌توانند رابطه میان افراد و گروه‌ها را سازماندهی کرده و به این ترتیب بر شبکه‌های اجرای جنگ نرم تأثیر بگذارند. شواهد نشان می‌دهد که رسانه‌ها، ماهیت بسیط دارند؛ به همین دلیل است که تصاویر می‌توانند نمادین جدیدی تولید کنند. این امر، زمینه‌های «کدگذاری ذهنی» در فضای اجتماعی را به‌وجود می‌آورد و از این طریق، تصاویر به حوزه‌های شبکه ارتباط اجتماعی منتقل می‌شود (Hollway, 1994:55).

ب) شاخص‌های سیاسی - فرهنگی جنگ نرم

جنگ نرم تحت تأثیر شاخص‌های متنوعی شکل می‌گیرد. در دوران جنگ سرد، موضوع‌های نظامی و راهبردی را می‌توان اصلی‌ترین عوامل و نشانه‌های رفتاری بازیگران دانست. روند یاد شده در شرایط جدید با تغییرات محتوایی همراه شده است. تغییرات شکل گرفته در ابزارهای ارتباطی را می‌توان یکی از عوامل مؤثر در ظهور عوامل جدید منازعه دانست. مؤلفه‌های سیاسی از طریق ابزارهای ارتباطی منتقل می‌شوند. هرگاه توزیع قدرت در دستور کار قرار گیرد، برای شکل‌گیری نشانه‌های جدید منازعه زمینه فراهم می‌شود.

نهاد‌های سیاسی و ساختمان قدرت در عصر جنگ نرم، مشروعیت و کارکرد خود را از دست داده‌اند؛ به گونه‌ای که فرایندهای سیاسی از تحول و دگرگونی فراگیرتری در مقایسه با قدرت باز تولید سیاسی برخوردارند. در این ارتباط در فضای تغییرات سریع قرار دارند، در نتیجه مشروعیت نهاد‌های سیاسی به سرعت در فضای چالش قرار می‌گیرد. چرخه غیر رسمی قدرت در چنین شرایطی از قابلیت و تأثیرگذاری بیشتری برخوردار می‌شود. به‌طور کلی می‌توان تأکید کرد که در شرایط جنگ نرم، چرخه رسمی قدرت، تحت فشار ناشی از پیچیدگی‌های ساختار اجتماعی و ارتباطی قرار می‌گیرد؛ احزاب و نهاد‌های سیاسی، کارکرد خود را برای کنترل محیط و سازماندهی برنامه‌های اجرایی از دست می‌دهند؛ گروه‌های اجتماعی با

رسانه‌ای، فرهنگی و اجتماعی است که جامعه یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش، رقیب را به انفعال یا شکست و می‌دارد (ماه پیشانیان، ۱۳۸۶).

تغییرات حاصل از تهدید نرم، ماهوی، آرام، ذهنی، تدریجی و نرم‌افزارانه است. این تهدید همراه با آرامش و خالی از روش‌های فیزیکی و با استفاده از شیوه القاء، مجاب‌سازی و اقناع و در بسترهای قانونی بدون ایجاد حساسیت و برانگیختن اعمال می‌شود. در مجموع می‌توان فهرست زیر را به‌مثابه نقاط افتراق تهدیدات سخت و نرم برشمرد.

۱. حوزه تهدید و جنگ نرم، حوزه اجتماعی، فرهنگی و سیاسی است.

۲. تهدید و جنگ نرم پیچیده و محصول پردازشی ذهنی نخبگان و اندازه‌گیری آن مشکل است.

۳. روش اعمال تهدید و جنگ نرم، بهره‌گیری از مدل‌های روان‌شناختی در تغییر رفتار، مجاب‌سازی به القاء و قانع‌سازی است.

۴. تهدید و جنگ نرم به دلیل ماهیت غیردینی و محسوس آن، اغلب فاقد عکس‌العمل است، یعنی مسالمت‌آمیز بوده و جنبه غیرخشونت‌ناهی دارد و بنابراین حوزه‌های سطحی - حمایتی را در جامعه و حکومت برنمی‌انگیزد.

۵. ارزیابی پیامدهای تهدید و جنگ نرم و تشخیص میزان شکست و پیروزی آن، بسیار سخت است (مرادی ۱۳۸۸: ۳۸ و ۹۹).

جنگ نرم امروزه با بهره‌گیری از حوزه‌هایی چون: دیپلماسی عمومی، دیپلماسی رسانه‌ای و مجازی (تصویرسازی)، تجربه کاملاً متفاوتی از رویارویی کشورها را به‌منصه ظهور رسانده است. در عصر حاضر، تصویرسازی موضوعیت یافته است، به این معنا که بازیگران سعی می‌کنند با استفاده از رسانه‌ها و فناوری‌های نوین، از رقیبان خود «تصویری مجازی» تولید کنند که امکان جایگزین شدن با واقعیت را داشته باشد (میلسن و همکاران، ۱۳۸۸: ۲۶). جنگ روانی، جنگ رایانه‌ای، جنگ سایبری و جنگ اطلاعاتی را از جمله مصادیق جنگ نرم به‌شمار می‌آورند (احمدزاده، ۱۳۸۸: ۴۴).

الف) تصویر سازی در جنگ نرم

تصاویر به عنوان ابزارهای انتقال نشانه‌های هنجاری و غیرهنجاری محسوب می‌شوند. این امر، ذهن شهروندان و

تنها ۲۵ میلیون کاربر دارند، همچنین حدود سی کشور در جهان است که واژه اینترنت در آنها واژه غریبی است. چون ضریب نفوذ اینترنت در این کشورها کمتر از یک درصد گزارش شده است. مؤسسه تحقیقاتی (OVUM) به‌تازگی کشورهایی را معرفی کرده که ضریب نفوذ اینترنت در آنها به سرعت در حال افزایش است. ایرلند، یونان، ترکیه، روسیه (مجیدی، ۱۳۸۸: ۱۲۵).

امروزه کاربرد اینترنت با زبان انگلیسی به‌گونه‌ای عجیب شده است که به نظر می‌رسد آنها اجزاء جدایی‌ناپذیر یکدیگرند. میلیون‌ها کاربر اینترنتی مجبورند برای استفاده از اینترنت با این زبان آشنا باشند. همچنین روابط بین‌المللی به‌طور معمول در سطح سازمان‌های بین‌المللی و منطقه‌ای براساس این زبان صورت می‌گیرد. اگرچه گسترده و سیطره زبان انگلیسی را می‌توان از ابزار موردی استعمار تلقی کرد که تهدیدی برای ارکان و شئون مختلف علمی، فرهنگی و سایر ابعاد آشکار و نهان آن کشورها به‌شمار می‌آید؛ ولی شبکه اینترنت در جهان با ارتباط تنگاتنگ بین این دو پدیده گسترش یافت. سرعت و گستره از ویژگی‌های منحصر به‌فرد اینترنت بوده که اطلاعات را می‌توان تقریباً فوری به هر جای دنیا ارسال کرد؛ از بین رفتن فاصله‌ها موجب افزایش تعداد کسانی شده است که می‌توانند درباره دیگر کشورها، کشور خود و نیز کسانی که روابط بین‌المللی را شکل می‌دهند اطلاعات به‌دست آورند (Kellerman, 2000).

ژوزف نای رشد استفاده از زبان انگلیسی را به عنوان زبانی برای ارتباطات فرامرزی این‌گونه توصیف می‌کند که این زبان به آمریکا قدرت نرم بخشیده است. «این قدرت و توان به شما امکان می‌دهد آن چیزی را که می‌خواهید بدون به‌کارگیری پول یا خشونت به دست آورید» (نامی، ۲۰۰۴: ۲). به‌نظر می‌رسد آمریکا از دو مزیت زبان انگلیسی به عنوان منبع قدرت نرم برخوردار است:

۱. زبان انگلیسی در نقش میانجی در دیپلماسی بین‌المللی.
۲. افزایش ارتباطات فرامرزی از طریق اینترنت به زبان انگلیسی (Cowan, 2000:211).

در این میان زبان شرط لازم ارتباط است؛ اما کلمات، نمادهای ریاضی یا حرکات فیزیکی بدون درک مشترک دو طرف ارتباط بی‌معنا خواهد بود. تفاوتی نمی‌کند که طرف‌های ارتباط

حمایت گروه‌های ذی‌نفوذ و رسانه‌ها، مطالبات خود را مطرح می‌کنند؛ در این فرایند، سیستم‌های تماس متنوع و فراگیری بین مردم و دولت ایجاد شده است که این امر از کورپوراتیسم تا مشارکت مستقیم شهروندان در تصمیم‌گیری‌ها دولتی را تحت تأثیر قرار می‌دهد. احزاب سیاسی در شرایط رقابت‌های متنوع و ساختار پیچیده، کارکرد تناقض‌آمیز دارند و به عبارتی؛ احزاب و نهادها در قالب چرخه‌های غیررسمی سیاسی ایفای نقش می‌کنند. (Wartberg, 1997:124) به همین دلیل است که ارتباطات، ماهیت دوگانه دارد. از یک سو، زمینه‌های هنجارسازی، قدرت‌سازی و تولید مشروعیت برای نظام سیاسی را فراهم می‌آورد؛ این امر به‌منزله جلوه‌هایی از قدرت نرم محسوب می‌شود و از سوی دیگر، منجر به مشروعیت‌زدایی می‌شود که در این صورت، زمینه برای شکل‌گیری فرایندهای منازعه‌آمیز ایجاد می‌شود (متقی، ۱۳۸۸: ۶۵).

عوامل مؤثر بر مجازی‌سازی

سرعت رشد پدیده‌های نوین تکنولوژیکی در کشورهای پیشرفته به‌مراتب بیش از کشورهای در حال توسعه و جهان سوم است. براساس آمار سازمان ملل متحد، تعداد کاربران اینترنت در جهان از مرز یک میلیارد نفر گذشته است و پیش‌بینی می‌شود این رقم تا سال ۲۰۱۱ به دو میلیارد نفر برسد. هم‌اینکه درصد کاربران اینترنت در آسیا ۳۶/۶ درصد، اروپایی ۲۷/۷ درصد، آفریقا ۳/۵ درصد، آمریکای شمالی ۱۸/۸ درصد، آمریکای جنوبی ۹/۷ درصد گزارش شده است (مجیدی، ۱۳۸۸: ۱۲۴). ایده اینترنت را نخستین بار در دهه ۱۹۶۰ سازمان پروژه‌های تحقیقاتی پیشرفته وزارت دفاع آمریکا مطرح کرد تا در صورت بروز جنگ هسته‌ای، شوروی سابق نتواند مخابرات آمریکا را اشغال یا نابود کند (کاستلز، ۱۳۸۰). بنابر آمارهای سال ۲۰۰۷ از مرکز اطلاعات شبکه اینترنت تا پایان سال گذشته (۲۰۰۷) تعداد کاربران اینترنت در این کشور به ۲۱۰ میلیون نفر رسید که این میزان پنج میلیون نفر کمتر از تعداد کاربران در آمریکا است (خبرگزاری مهر، ۲۵ آبان ۸۶).

در میان کشورهای عربی نیز، امارات متحده عربی در رتبه اول است، کویت جایگاه دوم را در اختیار دارد. تعداد ۳۵ کشور آفریقایی

ابعاد اجتماعی

موارد زیر از جمله آسیب‌های اینترنت در بعد اجتماعی است:

الف) ارتباطات نامتعارف میان جوانان: اینترنت به دلیل تسهیل ایجاد روابط دوستانه و عاشقانه، در زمینه‌های غیراخلاقی بسیار مورد توجه قرار گرفته و تا جایی که اینترنت موجب سهولت خیانت در روابط زناشویی و ایجاد روابط نامشروع می‌شود.

ب) جرائم رایانه‌ای و اینترنتی: به‌عنوان مثال شاید نفوذ به سایت بانک ملی ایران و شبکه شتاب یکی از مهمترین نشانه‌های آسیب‌پذیری از اینترنت است، گسترش شبکه‌های مجازی تجارت الکترونیک و آن‌چه به نام گلدکوئیست و پنتاگون و چند نام دیگر شناخته شده است.

ج) گسست میان نسلی: اینترنت شکاف میان نسل‌ها را بیشتر کرده است و اکنون شکاف میان نسل دوم و سوم علاقمند به اینترنت نیز آشکار شده، به‌گونه‌ای که هیچ یک زبان دیگری را نمی‌فهمند.

د) بی‌هویت‌سازی: با امکانات و گزینه‌های فراوانی که اینترنت در اختیار جوانان می‌گذارد، آنان به‌طور دائم با محرک‌های جدید و انواع مختلف رفتارها آشنا می‌شوند. این فضا، هویت نامشخص و اغلب متحولی را می‌آفریند، یعنی اینترنت یک صحنه اجتماعی است که فرد خود را در موقعیت‌های متنوع نقش‌ها و سبک‌های زندگی، قرار می‌دهد و از آن تأثیر می‌پذیرد.

ه) تهدید بنیان‌های خانواده: تغییر ارزش‌ها و هنجارهای اجتماعی به‌نوبه خود بنیان‌های خانوادگی را در معرض تهدید قرار می‌دهد.

و) شکل‌گیری خرده فرهنگ‌های مختلف: کارکرد غالب چت‌های اینترنتی در جوانان باعث گسسته شدن فرهنگ می‌شود.

ز) انتشار مطالبات قومی و منطقه‌ای و افزایش تحریک‌پذیری قومیت‌ها: خاصیت تأسیس سایت‌های قومی و راه‌اندازی وبلاگ‌های منطقه‌ای و انتشار برخی مطالب تحریک‌آمیز در سایت‌های اینترنتی قابلیت این رسانه و پدیده برای دامن زدن به مباحث مناقشه‌آمیز قومی را بالا برده است.

خواه به زبان انگلیسی یا ژاپنی صحبت کنند یا حتی با علائم ریاضی با یکدیگر ارتباط برقرار نمایند از آنجایی که اینترنت سریع‌تر از رشد فهم و درک کشورها نسبت به یکدیگر توسعه می‌یابد، بنابراین احتمال ارتباط نامتقارن را افزایش می‌دهد. در این ارتباط نامتقارن، کشورهای که فهم بیشتری دارند از قدرت نرم بیشتری برخوردار خواهند شد.

بنابراین وقتی زبان‌های ملی مختلف باشد، ارتباطات فرامرزی مستلزم آن خواهد بود که یک یا هر دو طرف ارتباط چند زبانی داشته (جهانی باشند) و سیاست خارجی را به زبان خارجی اداره کنند، بنابراین فناوری اینترنت بدون توجه به مرزهای ملی ارتباطات را امکان‌پذیر کرده است؛ ولی جامعه‌شناسی اینترنت این‌گونه نیست، توانایی کاربران در گفتگو با یکدیگر کارکرد جمعیت یک کشور نیست؛ بلکه نشانگر تعداد کاربران سهیم در فهم یک زبان مشترک است (مرادی، ۱۳۸۸: ۳۴۶-۳۴۷).

آسیب‌های اینترنت در فضای نامتعادل اجتماعی:

ابعاد امنیتی - اطلاعاتی

در بعد امنیتی - اطلاعاتی گزینه‌های فراوانی برای بررسی وجود دارد:

الف) جاسوسی اینترنتی: دسترسی آسان به سایت‌های جاسوسی آمریکا، اسرائیل و کشورهای دیگر امکان ارسال و دریافت ایمیل به هر نقطه از دنیا و غیرقابل کنترل بودن داده‌های مبادله شده، فریب انجام جاسوسی از طریق اینترنت را بالا برده است. در واقع، این دسترسی، انتقال اطلاعات و انتشار هرگونه اطلاعات طبقه‌بندی شده بر روی اینترنت را فراهم آورده است.

ب) کاهش اقتدار سیستم امنیتی و اطلاعاتی: به دلیل امکان نشر بدون واژه و فارغ از امکان شناسایی از سوی اینترنت، سیستم امنیتی و اطلاعاتی، اقتدار سنتی خود در کنترل افکار عمومی و یا اشراف اطلاعاتی معمول را از دست داده‌اند و حتی گاه خود سیستم‌های اطلاعاتی و امنیتی مورد دستبرد اطلاعاتی قرار می‌گیرند.

ج) آموزش مخرب: از جمله این آموزش‌ها، آموزش‌های تروریسم، آموزش مصرف مواد مخدر و آموزش فرق ضاله و مانند آن است.

ابعاد سیاسی

(ب) افزایش ضریب نفوذ جریان‌های معاند،
(ج) افزایش همگرایی گروه‌های داخلی و خارجی همفکر
علیه نظام.

(الف) ایجاد گروه‌های سیاسی مجازی: از طریق اینترنت، گروه‌های سیاسی خاصی به وجود می‌آوردند که فقط بر روی شبکه اینترنت وجود دارند و از آن طریق می‌توان به آنها دست یافت.

ابعاد فرهنگی

اینترنت در بعد فرهنگی هم به صورت‌های زیر آسیب رسانده است:

(ب) اختلال در روند کنترل جریان اطلاع‌رسانی سیاسی: رسانه‌ها و نشریات الکتریکی بدون کسب اجازه از نظام منتشر شده، روند اطلاع‌رسانی رسمی - سیاسی را مختل می‌کنند.

(الف) کاهش نفوذ رسانه‌های ملی و داخلی: به همان اندازه که رسانه‌های خارجی و رسانه‌های اینترنتی مخاطب جدید کسب می‌کنند همان اندازه هم از تعداد مخاطبان رسانه‌های داخلی کاسته می‌شود.

(ج) انتقال مستقیم اندیشه‌ها و دیدگاه‌های جریان‌های معاند به داخل: اگر تا دیروز برای انتقال افکار و دیدگاه‌های معاندان نظام به داخل فقط نشریات مکتوب وجود داشت، امروزه از طریق اینترنت، گروه‌های خبری و خبرنامه‌ها الکترونیک، امکان انتقال مستقیم اندیشه‌های معاندان به داخل وجود دارد.

(ب) ایجاد محرک‌های قوی برای تبادلات فرهنگی
غیرقابل کنترل:

(د) ایجاد گروه‌های فشار و ذی‌نفوذ مجازی
(ه) کارکردهای مشروعیتی: از طریق برگزاری فراندوم‌های اینترنتی و سیستم‌های نظرسنجی اینترنتی، این ابزار امکان اعطا یا سلب مشروعیت از عملکرد سیاسی سیستم را فراهم کرده است.

در واقع با وجود اینترنت بسیاری از محصولات فرهنگی که ماده اولیه آنها اطلاعات هستند مثل کتاب، مقاله، موسیقی، فیلم، بدون مانع مبادله می‌شود. این به هم آمیختگی فرهنگی بویژه میان ایرانیان داخل و خارج کشور نیز قابل کنترل است.

(و) دموکراسی دیجیتال: از مهمترین آثار پیدایش جامعه اطلاعاتی، شکل‌گیری نفع خاصی از دموکراسی است که در دوره‌های پیش، مسبوق به سابقه نیست. در حال حاضر دموکراسی دیجیتالی می‌تواند به طیف وسیعی از کاربردهای فناورانه و از جمله پارلمان‌های مردمی تلویزیونی و یا هیئت‌های منصفه شهروندان اطلاق می‌شود که از راه پست الکترونیکی با گروه‌های مخاطب ارتباط برقرار می‌کنند، بدون آنکه نیازی به حضور فیزیکی افراد باشد.

(ج) بسترسازی بیشتر برای تهجم فرهنگی،
(د) انتقال هنجارها و فرم‌های ارزشی و اخلاقی غربی،
(ه) چالش‌های انتقادی در مباحث دینی و مذهبی،
(و) جایگزینی رسانه‌ای: (مجیدی، ۱۳۸۴: ۱۲۷-۱۲۵).

بازی‌های رایانه‌ای ابزار جنگ نرم در فضای سایبری (عملیات روانی)
بازی‌های رایانه‌ای بیشتر در عملیات روانی استراتژیک قرار می‌گیرند. این عملیات، عموماً برای پیشبرد اهداف گسترده یا بلندمدت و در هماهنگی با طرح‌ریزی استراتژیک کلی طراحی شده و به‌طور معمول دارای تأثیراتی در آینده دور است. بیشتر بازی‌های رایانه‌ای به‌منظور تسریع خط‌مشی‌ها، اهداف و مقاصد سیاسی کشور خودی برای مخاطبان و ارائه استدلال‌هایی با هدف پشتیبانی از آن خط‌مشی‌ها تولید و به صحنه بین‌المللی عرضه شده است (مرادی، ۱۳۸۱: ۳۲۵).

(ز) مکانیسم‌های جدید شایعه‌سازی و بی‌اعتبارسازی مرزها.

ابعاد بین‌الملل

اهداف عملیات روانی استراتژیک عبارتند از:
(الف) تشریح خط‌مشی‌ها، اهداف سیاسی کشور خودی برای مخاطبین و ارائه استدلال‌های پشتیبانی از آن خط‌مشی‌ها،

اینترنت در ابعاد بین‌الملل هم به صورت‌های زیر آسیب رسانده است:

(الف) ورود بازیگران جدید در عرصه مناسبات داخلی،
مثال: تغییر نام خلیج فارس از طرف نشریه نشنال ژئوگرافیک، نمونه‌ای از ورود بازیگران بین‌المللی به عرصه مسائل داخلی است،

می‌توان ویروس‌های رایانه را ساخت و از طریق خطوط تلفن، کابل و ارتباط بی‌سیم آن را ارسال کرد.

ب) سایبر تروریسم ناشناخته‌تر از روش‌های تروریسم کلاسیک است، مانند بسیاری از کاربران اینترنت تروریست‌ها از اسامی مستعار استفاده می‌کنند و به یک سایت به‌عنوان کاربر مهمان و ناشناس وصل می‌شوند.

ج) تنوع و تعداد حملات بسیار زیاد است، سایبر تروریسم می‌تواند شبکه‌های دولتی یا رایانه‌های دولتی، شخصی، خدمات عمومی، هوایی را مورد حمله قرار می‌دهد. مطالعات نشان داده است، شبکه‌های برق و خدمات اضطراری در برابر حملات آسیب‌پذیر هستند.

د) سایبر تروریسم را می‌توان از راه دور هدایت کرد.

ه) سایبر تروریسم توانایی زیادی در جهت جذب تعداد زیادی از مردم را به خود دارد.

و) روش‌های کلاسیک تروریستی اهداف تروریست‌ها را برآورد نمی‌کند (cyber - chalany. Blogfa.com).

بسترهای فراهم‌کننده سایبر تروریسم

الف) به روز نکردن اطلاعات به‌وسیله گردانندگان سایت‌ها،
ب) در دسترس نبودن اطلاعات و به این دلیل که کاربران خواسته و ناخواسته سعی در دسترسی به اطلاعات و دستکاری و به روز کردن آن‌ها دارند،

ج) رازدار نبودن مدیران سایت و فاش‌سازی اطلاعات به‌وسیله آن‌ها،
د) خرابی فیزیکی سیستم IT یا سرور خدمات‌دهنده (عزیزی، ۱۳۸۸: ۱۲۳).

از مهمترین گروه‌های رایانه‌ای که از پدیده سایبر تروریسم علیه ایران و مسلمانان استفاده می‌کنند، سایت‌هایی است که طرفدار اسرائیل‌اند. این گروه به سایت‌های حامی سازمان‌های به‌زعم آنها تروریستی مانند حمام و حزب‌الله حمله می‌کنند، از جمله هاگانا وب سایت هاگانا به‌وسیله فردی آمریکایی یهودی‌الاصل که Andrew Aaron Weisburd خوانده می‌شود و در ایالات متحده ساکن است، تأسیس شده است. وب سایت هاگانا در طول دو سال و نیم فعالیت خود صدها وب سایت اسلامی را مورد تعقیب قرار داده و بیشتر از ۵۰۰ وب سایت را از راه اجبار شرکت‌های میزبانی و تهدید آنها به تعطیلی کشاند. وب سایت هاگانا اهداف تخریبی خود را با

برانگیختن افکار عمومی به طرفداری یا خصومت علیه یک عملیات نظامی،

ج) پشتیبانی از تحریم‌های اقتصادی و دیگر اشکال غیرقهرآمیز اعمال فشار علیه دشمن،

د) غرب در این بازی‌ها از سه روش افکار، غریب و تحریف استفاده می‌کنند. (Aspxtele3 minhanblog. Com 39).

سایبر تروریسم یا تروریسم اینترنتی

واژه سایبر تروریسم نخستین بار از طرف کالین باری (Collin Barry) و در دهه ۱۹۸۰ مطرح شد؛ ولی گفته می‌شود جامع‌ترین تعریف از سوی «دوروتی دلینگ» استاد علوم رایانه‌ای دانشگاه جرج تاون ارائه شده است: «سایبر تروریسم حاصل تلاقی تروریسم و فضای مجازی است. سایبر تروریسم بیشتر به‌معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌هاست، هنگامی که به‌منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود». اساسی‌ترین روش‌های سایبر تروریسم عبارتست از: هک کردن، ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات (عزیزی، ۱۳۸۸: ۱۲۲).

سایبر تروریسم تاریخچه طولانی ندارد؛ بلکه در سال ۱۹۸۲ هک‌های طرفدار دولت پاکستان با نام «باشگاه هک‌های پاکستانی» به کامپیوترهای هند حمله کردند. در سال ۲۰۰۰ سایت حزب‌الله لبنان که یک سایت ضدصهیونیستی است، به‌وسیله یک گروه هکر اسرائیلی هک شد و پرچم و سرود ملی اسرائیل روی آن قرار گرفت. در مقابل حزب‌الله لبنان در یک ضدحمله به وب‌سایت اصلی دولت اسرائیل و وب سایت وزارت خارجه اسرائیل حمله کرده و آن را هک کردند (مجیدی، ۱۳۸۸: ۱۲۷).

جذابیت سایبر تروریسم

دلایل زیادی وجود دارد که سبب می‌شود سایبر تروریسم برای تروریست‌ها جذاب باشد.

الف) سایبر تروریسم ارزان‌تر از روش‌های تروریستی متداول (کلاسیک) است. تنها چیزی که مورد نیاز است یک رایانه شخصی متصل به اینترنت است، نیازی به خرید اسلحه نیست،

کمال وقاحت ابراز می‌کند (مجیدی، ۱۳۸۱: ۱۲۸).

نتیجه‌گیری

آنچه مسلم است انقلاب فناوری نظامی، وضعیت جنگ سنتی را از ریشه دگرگون کرده، اگرچه آن را به پایان نبرده است، روشن است که نوآوری‌های فناوری به تنهایی نمی‌تواند این انقلاب را به وجود آورد. رسانه‌های گروهی منظره‌ای بدون خونریزی، انسانی، بهداشتی و پاکیزه را از جنگ‌ها منتشر کرده و می‌توانند شرایط جنگ را از طریق تبدیل و یا تخفیف مرگ در طی جنگ‌ها، شبیه‌سازی، مسافت‌سازی، فضیلت ضدجلوه‌دادن جنگ، دگرگون‌سازی طبیعت جنگ، راه یافتن جنگ مجازی به همه صفحه‌های نمایشی، رایانه (اینترنت) را تغییر دهند.

امروزه رسانه‌های گروهی از جمله اینترنت با بکارگیری جنگ نرم، عملیات روانی و تبلیغات بیشتر از جنگ و در طی جنگ، بعد جدیدی از جنگ نرم‌افزاری یا مجازی را در صحنه داخلی و خارجی پدید آورده است که برخلاف گذشته صرفاً به سخت‌افزار و نبرد فیزیکی متکی نیست و براین اساس در این فضای سایبری (به‌خصوص سایبر تروریستی) سازوکارهای متعددی را می‌توان بعنوان راهبرد دفاعی در پیش گرفت از جمله آموزش، سازوکارهای حقوقی و تقویت دفاعی را نام برد.

مهمترین مرحله در جلوگیری از سایبر تروریسم اینترنتی، آموزش است. این آموزش شامل آموزش عمومی (آموزش مقامات سیاسی) امنیتی و پلیسی است، نه تنها مردم عادی بلکه احتمالاً بسیاری از مقامات، هیچگونه اطلاعاتی در مورد حملات سایبر اینترنتی و چگونگی آن ندارند. باید در مورد ایمن کردن کاربر اینترنت شخصی آنها را باید متقاعد کرد و با آگاهی دادن به مردم آنها را وادار کرد تا تمهیدات لازم برای مقابله با سایبر تروریسم را اعمال کنند.

دوم سازوکار حقوقی: در مرحله بعد باید سازوکار حقوقی و قضایی مناسبی را برای مبارزه با سایبر تروریسم ایجاد کرد. وجود خلأهای قانونی نیروهای امنیتی و قضایی را در مقابل با سایبر تروریسم دچار سردرگمی می‌کند و توانایی اقدام به‌موقع و مناسب را از آنان می‌گیرد. ایجاد دادگاه‌های ویژه جرائم اینترنتی قدم مهمی در مبارزه با سایبر تروریسم است، چرا که رسیدگی به

این جرائم را آسانتر و سریع‌تر می‌کند و با به خطر انداختن امنیت مجرمان گام مؤثری در کاهش حملات تروریستی خواهد بود.

در نهایت تقویت دفاعی که با ایجاد سازمان‌های مسئول مقابله با سایبر تروریسم (سازمان‌هایی که مسئولیت آنها مطالعه و تحقیق و مقابله با حملات سایبر باشد) را نام برد و روش دفاعی دیگر عبارتست از: سخت کردن حملات از طریق تقویت فناوری امنیتی و تعریف روز آمد و بررسی‌های رایانه‌ای، استفاده از نرم‌افزارهای ضد ایرانی، استفاده از رمزهای عبور قوی و دیوار آتش است.

منابع:

- احمدزاده کرمانی، روح الله. (۱۳۸۸). درآمدی بر ماهیت‌شناسی جنگ نرم و پس از انقلاب اسلامی ایران، فصلنامه مطالعاتی بسیج، شماره ۴۳.
- احمدزاده کرمانی، روح الله، محمدصادق اسماعیلی. (۱۳۸۷). فرهنگی شدن سیاست خارجی: رویکردی نرم‌افزارانه، تهران، پژوهشکده مطالعات و تحقیقات بسیج دانشگاه امام صادق (ع).
- افتخاری، اصغر. (۱۳۸۷). قدرت نرم، تهران، پژوهشکده مطالعات و تحقیقات، بسیج و امام صادق (ع).
- خبرگزاری مهر، ۲۵ آبان ۱۳۸۶.
- عزیزی، مرتضی. (۱۳۸۸). «سایبر تروریسم یا تروریسم اینترنتی» معاونت سیاسی نهاد نمایندگی مقام معظم رهبری در دانشگاه.
- کاستلز، مانوئل. (۱۳۸۰). عصر اطلاعات، فرهنگ ظهور جامعه شبکه‌ای؛ (ترجمه: احمد علیقلیان، افشین خاکباز)؛ تهران: انتشارات طرح نو.
- ماه پیشانیان، مهسا. (۱۳۸۶). «راهکارهای آمریکا برای جنگ نرم با جمهوری اسلامی ایران» فصلنامه عملیات روانی، ش ۱۸.
- متقی، ابراهیم. (۱۳۸۸). «مدیریت جنگ نرم در فضای عدم تعادل امنیتی» فصلنامه مطالعات بسیج، ش ۴۳.
- مجیدی، عبدال... (۱۳۸۱). «نقش رسانه‌های اینترنت در ناامنی‌های اجتماعی» تهران، معاونت سیاسی نهاد نمایندگی مقام معظم رهبری.
- مرادی، حجت‌الله. (۱۳۸۸). «قدرت جنگ نرم از نظریه تا عمل» تهران: انتشارات ساقی.
- نائینی، علی‌محمد. (۱۳۸۷). قدرت و تهدید نرم در مطالعات امنیتی با مجموعه مقالات قدرت نرم، جلد اول؛ پژوهشکده مطالعات بسیج.
- نای، جوزف. (۱۳۸۲). «قدرت نرم» ترجمه محمد حسینی مقدم، فصلنامه راهبرد، ش ۲۹ - Aspotele 3xmihan.
- Cowan, R./ David/p. and Foray, D. (2000) the Explicit Economics of knowledge codification and Tacitness. Industrial and corporate change 9: 211-253.
- Hollway, W (1994). Power and Social Relations, London, sage.
- Kellerman, A. (2002) The Internet on Earth: Geography of Information (John wiley: New York).
- Warterberg, E (1992). Rithinking of Power, Albany, State University of New York.
- Cyber-chalany.blogfa.com