

تأثیر شبکه‌های اجتماعی مجازی بر امنیت ملی

کد موضوعی: ۲۶۰

شماره مسلسل: ۱۲۲۳۶

بهمن‌ماه ۱۳۹۰

به نام خدا

فهرست مطالب

| | |
|----|---|
| ۱ | چکیده |
| ۱ | مقدمه |
| ۳ | فضای مجازی |
| ۴ | تأثیر شبکه‌های اجتماعی بر امنیت |
| ۱۰ | شبکه‌های اجتماعی در خدمت اهداف سیاسی آمریکا |
| ۱۴ | شبکه‌های اجتماعی و امنیت ملی جمهوری اسلامی |
| ۱۹ | نتیجه‌گیری |
| ۲۲ | پی‌نوشت‌ها |



تأثیر شبکه‌های اجتماعی مجازی بر امنیت ملی

چکیده

امروزه شبکه‌های اجتماعی مجازی تبدیل به وسایل ارتباط و تعامل جوامع انسانی شده‌اند و هر روز بر تعداد و اعضای آنها افزوده می‌شود. وجود شبکه‌های اجتماعی مجازی امکانات جدیدی را برای افراد در جامعه ایجاد کرده و آنها را قادر ساخته است تا در هر مکانی با اعضای دیگر شبکه ارتباط حاصل کرده و به راحتی ایده‌ها، باورها، خاطره‌ها و تصاویر ویدئویی و عکس‌های خود و یا دیگران را با اعضای شبکه به اشتراک بگذارند. هرچند که این امکانات، بشر امروزی را توانمندتر از گذشته کرده است، اما آسیب‌هایی را نیز بر زندگی او بار می‌کند. چنان‌که شبکه‌های اجتماعی تبعاتی را برای امنیت اعضای خود به وجود آورده‌اند. در این گزارش سعی شده است ضمن ارائه توصیفی از طرز کار این شبکه‌ها، تهدیداتی که از جانب آنها بر امنیت جامعه و کشور وارد می‌شود بررسی و راهکارهایی برای استفاده از فرصت‌ها و جلوگیری از تهدیدات آنها ارائه شود.

مقدمه

تکنولوژی‌های ارتباطی - به‌ویژه تکنولوژی‌های ارتباطی دیجیتالی - مرزها را کمرنگ، جهان را کوچک، سرعت ارتباطات را تشدید و دامنه ارتباطات را گسترده کرده‌اند. اکنون یک فرد - به‌عنوان واحد اولیه جامعه و بسیار ناتوان‌تر از سطوح دیگر - به راحتی می‌تواند در هر نقطه از جهان و در یک چشم به هم زدن با هر فرد دیگری ارتباط مجازی برقرار کند. اهمیت این نوع ارتباط، زمانی روشن می‌شود که بدانیم همه افراد در جهان می‌توانند با سازمان‌ها، ادارات، آژانس‌های خبری، سرویس‌های جاسوسی و دولت‌ها و همه آنها با یکدیگر ارتباط بدون واسطه داشته باشند آن هم در مدت کوتاهی که از زمان ارتباط‌گیری در یک دهکده نیز کمتر است. اندک بودن زمان لازم برای ایجاد ارتباط از این سر تا آن سر جهان باعث شده است مرزها و فاصله‌ها بی‌معنا شوند و جهان به صورت دهکده‌ای کوچک درآید. این موضوع را اندیشمندان، فشردگی زمان و مکان نامیده‌اند.

با این توصیف از جهان، امنیت که لازمه‌اش وجود مرزهای قابل کنترل است چه وضعیتی پیدا می‌کند و تبعات ارتباطات گسترده جهانی بر امنیت در داخل کدامند؟ فضای مجازی و ازجمله

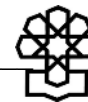
شبکه‌های اجتماعی مثل فیس‌بوک و توییتر که امکان هم‌پیوندی‌های جهانی را دو چندان کرده‌اند چه تأثیراتی بر امنیت داخلی دارند و چگونه می‌توان از تبعات منفی فعالیت آنها جلوگیری کرد؟

برای ارائه توصیف مجملی از وضعیت شکننده امنیت در دنیای به هم پیوسته امروزی نقل قولی از کاستلز وافی به مقصود خواهد بود. کاستلز در جلد دوم از کتاب سه‌جلدی خود، عصر اطلاعات، می‌نویسد: «جهانی شدن و اطلاعاتی شدن که به دست شبکه‌های ثروت، تکنولوژی و قدرت انجام می‌گیرند، جهان ما را دگرگون می‌سازند. این دو فرآیند، توان خلاقیت فرهنگی و توانایی ارتباطی ما را تقویت می‌کنند. در عین حال آنها حق انتخاب را از جوامع سلب می‌کنند و از آنجا که نهادهای دولت و سازمان‌های جامعه مدنی بر پایه فرهنگ، تاریخ و جغرافیا استوارند، شتاب گرفتن ضرب‌آهنگ تاریخ و انتزاعی شدن قدرت در شبکه‌ای از رایانه‌ها، مکانیسم‌های موجود کنترل اجتماعی و باز نمود سیاسی را نابود می‌سازد. مردم سراسر جهان به استثنای معدود نخبگان جهان‌شهری، از فقدان کنترل بر زندگی‌شان، محیط‌شان، شغل‌شان، اقتصادشان، دولت‌شان، کشورشان و نهایتاً بر سرنوشت کره خاک دل چرکین‌اند».^(۱)

چنان‌که ملاحظه می‌شود کاستلز در عین حال که به تقویت توان خلاقیت فرهنگی و توانایی ارتباطی بشر در سایه تکنولوژی‌های ارتباطی جدید اشاره دارد از تضعیف مکانیسم‌های کنترل اجتماعی و نیز سلب حق انتخاب از جوامع گله می‌کند.

در این گزارش، بدون اینکه بخواهیم ظرفیت‌های بالای فضای مجازی برای زندگی بشر را نادیده بگیریم، درصددیم تا تأثیر آن را بر امنیت داخلی مورد بررسی قرار دهیم. مطمئناً در دنیایی که قدرت‌های سلطه‌گری مثل آمریکا در پی گستردن سلطه فرهنگی و سیاسی خود هستند، ابزارهای ارتباطی و اطلاعاتی جدید، می‌توانند کمک مؤثری برای رسیدن به اهداف سلطه‌گرایانه آنها باشند. این قدرت‌های سلطه‌گر می‌توانند برای رسیدن به اهداف خود از این ابزارها استفاده کرده و امنیت کشورهای دیگر را به خطر اندازند. امکان عملی شدن چنین اهدافی برای سلطه‌گران زمانی قابل باورتر است که از یاد نبریم که اکثر ابزارهای ارتباطی و اطلاعاتی موجود ابتکارات و اختراعات آنهاست و آنها در بدو اختراع چنین ابزارهایی از آنها برای اهداف سیاسی و نظامی استفاده کرده‌اند.

این گزارش به بررسی جوانب امنیتی فضای مجازی و مشخصاً شبکه‌های اجتماعی با تأکید بر فیس‌بوک و توییتر خواهد پرداخت.



فضای مجازی

وقتی از فضای مجازی صحبت می‌شود، اغلب مردم به رایانه‌ای فکر می‌کنند که به اینترنت متصل است در حالی که این فقط بخش بسیار کوچکی از فضای مجازی را تشکیل می‌دهد. فضای مجازی در واقع نامی است که تعداد زیادی از کاربردهای امروز فناوری‌های جدید ارتباطی را دربرمی‌گیرد. فضای مجازی یک شبکه گسترده جهانی است که شبکه‌های مختلف رایانه‌ای را در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر وصل می‌کند. فناوری‌های ارتباطی راه دور، اساس فضای مجازی را تشکیل می‌دهند.^(۲) از جمله رسانه‌هایی که در فضای مجازی و از طریق اینترنت، افراد انسانی و در واقع اجزای اجتماعات بشری را به هم متصل می‌گرداند شبکه‌های اجتماعی (مجازی) هستند.

شبکه‌های اجتماعی مجازی، نسل جدیدی از وب‌سایت‌های اینترنتی هستند. در این وب‌سایت‌ها، کاربران اینترنتی حول محور مشترکی به صورت مجازی جمع می‌شوند و اجتماع‌های آنلاین را تشکیل می‌دهند. هزاران شبکه اجتماعی در اینترنت فعال هستند که هرکدام بر مبنای موضوع خاصی راه‌اندازی شده‌اند.^(۳) این شبکه‌های اجتماعی در عین حال که فضاهایی هستند که در آنها افراد، دوستان جدیدی پیدا می‌کنند و یا دوستان قدیمی خود را در جریان تغییرات زندگی‌شان قرار می‌دهند، مکان‌هایی برای تبادل نظر هستند که در آنها جوانان عقاید و نظرات خود را با هم به اشتراک می‌گذارند. این قابلیت که یک جوان بتواند با امثال خود در کشورهای دیگر ارتباط برقرار کند باعث می‌شود تا این شبکه‌ها به مکانی برای معرفی و مورد بحث و بررسی قرار دادن ایده‌های جدید تبدیل شوند.^(۴) از جمله شبکه‌های اجتماعی مجازی که در سال‌های اخیر توانسته‌اند کاربران و اعضای زیادی را به سوی خود جلب کنند، فیس‌بوک،^۱ توییتر،^۲ مای اسپیس،^۳ اورکات،^۴ فرنداستر^۵ و فلیکر^۶ را می‌توان نام برد.

شبکه‌های اجتماعی را می‌توان به دو گروه عمومی و تخصصی تقسیم کرد. در شبکه‌های اجتماعی عمومی، کاربران اینترنتی با انگیزه‌ها و اهداف مختلف حضور دارند و شبکه‌سازی مجازی‌شان را از طریق وب‌سایت‌ها دنبال می‌کنند، ولی شبکه‌های اجتماعی خاص حول موضوعی ویژه شکل گرفته‌اند و تعداد کاربران‌شان نیز کمتر است. فیس‌بوک، اورکات، مای اسپیس و توییتر مهم‌ترین شبکه‌های اجتماعی عمومی در دنیای اینترنت هستند. در این شبکه‌ها، هر نوع کاربری

1. Face Book
2. Twitter
3. My Space
4. Orkut
5. Friendster
6. Fliker

حضور دارد و اغلب دوستان و آشنایان آنلاین را می‌توان در آنها پیدا کرد. تعداد کاربران معروف‌ترین این نوع شبکه‌ها اغلب به چند صد میلیون نفر می‌رسد. علاوه بر اینها، شبکه‌های اجتماعی خاصی نیز وجود دارند که بر محوریت موضوعی مشخص فعالیت می‌کنند که «ایست اف ام»^۱ از جمله معروف‌ترین آنهاست که علاقمندان به موسیقی را گرد هم جمع کرده و «فلیکر» که وب‌سایتی برای علاقمندان به عکاسی است.^(۵)

از جمله شبکه‌های اجتماعی که امروزه تأثیر زیادی در زندگی افراد به‌ویژه جوانان دارند، فیس‌بوک و توییتر را می‌توان نام برد. این دو شبکه اجتماعی، شبکه‌هایی عمومی محسوب می‌شوند و کاربران آنها در صفحات مختص خودشان اطلاعات مربوط به خود و یا جامعه خود و حتی اطلاعات مربوط به جامعه جهانی را به اشتراک و بحث عمومی می‌گذارند. اهمیت این دو شبکه، به‌ویژه برای گزارش حاضر، از آن جهت است که آنها در سال‌های اخیر و به‌ویژه در ماه‌های گذشته در بسیج اقشار مختلف مردم، برای فشار آوردن بر دولت‌ها مؤثر بوده‌اند. به‌عبارت دیگر آنها به پایگاه‌هایی برای جنبش‌های سیاسی و اجتماعی تبدیل شده‌اند. اهمیت پرداختن به این شبکه‌های اجتماعی زمانی دو چندان می‌شود که استفاده‌های سیاسی دولت‌های سلطه‌گر و سازمان‌های جاسوسی دولتی و سازمان‌های تروریستی از این شبکه‌ها، در جهت ایجاد ناامنی و بی‌ثباتی سیاسی و تغییر فرهنگ و هویت ملی، را مورد توجه قرار دهیم. در این گزارش به دنبال بررسی تأثیر شبکه‌های اجتماعی مجازی بر امنیت داخلی کشورها، به‌ویژه ایران، با تأکید بر دو شبکه اجتماعی فیس‌بوک و توییتر هستیم.

تأثیر شبکه‌های اجتماعی بر امنیت

تأمین امنیت مهمترین دلیل وجودی دولت است. دولت‌ها با هر مکانیسمی که به‌وجود آمده باشند تأمین امنیت را پشتوانه مشروعیت خود قرار می‌دهند. حتی دولت مستبد و ستمگری که به اتباع خود ظلم کرده و به‌جای امنیت، رعب و وحشت در بین مردم ایجاد می‌کند، این کار را به بهانه ایجاد امنیت انجام می‌دهد. چنین دولتی هر فرد یا گروهی را که رقیب یا دشمن خود بداند با برچسب «مخل امنیت و ثبات ملی» معرفی کرده و به روش‌های گوناگون سرکوب می‌کند.

تعاریف گوناگونی از امنیت ارائه شده است. از یک لحاظ امنیت بر «وضعیتی» اطلاق می‌شود که در آن نسبت به منافع بازیگر «تهدیدی» از سوی دیگران وجود نداشته باشد یا در صورت وجود تهدید، امکان مدیریت آن برای بازیگر تهدیدشونده حاصل باشد. تعریف مذکور تعریفی سلبی است



و بر نبود تهدید تأکید می‌کند. اما تعریف دیگری که «ایجابی» است نبود تهدید را تنها «شرط لازم» امنیت می‌داند و عامل اصلی در تحقق امنیت را عنصر «رضایت» می‌نامد. در این تعریف امنیت وضعیتی است که در آن بین «خواسته‌ها» از یکسو و «داشته‌ها» ازسوی دیگر نسبتی متعادل وجود دارد.^(۶)

روشن‌ترین و ساده‌ترین تعریف امنیت همان نبود تهدید و به عبارت دیگر در امان بودن نسبی تمامی نیازها و ارزش‌های حیاتی مردم در برابر تهدیدات است.^(۷)

امنیت در ابعاد گوناگونی قابل بحث است از جمله: امنیت نظامی، امنیت اقتصادی، امنیت منابع و محیط زیست، امنیت فرهنگی و امنیت سیاسی. در همه این حوزه‌ها نبود تهدید منجر به وجود امنیت و برعکس وجود تهدید منجر به نبود امنیت می‌شود. همچنین امنیت در سطوح مختلفی مانند سطح فرد، جامعه، کشور، منطقه و جهان مورد بررسی قرار می‌گیرد.

مقوله دیگری که در امنیت مورد توجه قرار دارد نوع امنیت و یا نوع نبود امنیت - که تهدید نامیده می‌شود- است. از این لحاظ امنیت را به دو نوع عمده «سخت» و «نرم» تقسیم می‌کنند. تهدید سخت با دو مؤلفه خشونت‌آمیز بودن در روش اقدام و به بار آوردن نتایج سخت‌افزاری تعریف می‌شود. این نوع تهدید اغلب با ابزارها و تجهیزات مرگبار انجام شده و نتیجه آن تخریب، انهدام، کشتار و وحشت‌آفرینی است^(۸) و اما «تهدید نرم مجموعه اقداماتی است که باعث دگرگونی هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام سیاسی می‌شود». تهدید نرم نوعی سلطه در ابعاد حکومت، اقتصاد و فرهنگ است که از طریق استحاله الگوهای رفتاری در این حوزه‌ها، ایجاد شده، نمادها و الگوهای نظام سلطه جایگزین آن می‌شود.^(۹)

جوزف نای، کشورهای دارای قدرت نرم را که بتوانند امنیت سایر کشورها را به صورت «نرم» مورد تهدید قرار دهند با سه ویژگی مشخص می‌کند:

۱. فرهنگ و عقاید حاکم بر آنها به هنجارهای متداول و مسلط بر جهان نزدیک است.
 ۲. ابزارهای ارتباطی متعدد و مؤثری در اختیار دارند و از این طریق می‌توانند به گفتمان و چارچوب‌های جهانی شکل داده و یا آنها را تغییر شکل دهند.
 ۳. به واسطه سیاست‌ها و رویه‌های داخلی و بین‌المللی صاحب اعتبار و شهرت هستند.
- نای، معتقد است قدرت نرم صرفاً توانایی انجام کار یا توانایی کسب نتایج دلخواه نیست، بلکه عبارت از توانایی شکل دادن یا تغییر شکل دادن ترجیحات و اولویت‌های دیگران است به گونه‌ای که آن‌گونه که ما می‌خواهیم فکر یا رفتار کنند. بنابراین قدرت نرم نزد بازیگرانی است که بدون استفاده از زور و اجبار نتایج دلخواه را می‌گیرند؛ چون سیاست‌ها و ارزش‌های آنها برای دیگران جذابیت دارد.^(۱۰)
- امروزه دانشمندان حوزه امنیت، بیشتر تهدیدات امنیتی را تهدیدات نرم می‌دانند و علاقمندند تا

این بعد امنیت را بیشتر مورد توجه و بررسی قرار دهند. از جمله ابزارهایی که تهدید نرم از طریق آن اعمال می‌شود رسانه‌ها - اعم از دیداری و شنیداری - هستند. اما در میان رسانه‌ها اینترنت و به‌ویژه در دهه اخیر شبکه‌های اجتماعی جایگاه بارزی در اعمال تهدید و نیز در تضمین امنیت پیدا کرده‌اند. از آنجا که امنیت و تهدید رابطه‌ای معکوس با یکدیگر دارند آنکه امنیت دیگران را تهدید می‌کند از امنیت نسبی برخوردار است و آنکه مورد تهدید قرار می‌گیرد از امنیت نسبتاً کمتری برخوردار است و به‌عبارت دیگر احساس عدم امنیت می‌کند. شاید این موضوع - وجود رابطه‌ای معکوس بین امنیت و تهدید - موجب می‌شود که کشورها هرگز دست از اعمال تهدید نرم و در واقع تلاش برای کسب امنیت برندارند.

شبکه‌های اجتماعی مانند سایر ابزارهای تهدید نرم با تغییر ذهنیت افراد از طریق اقناع و رضایت برای صاحبان خود امنیت و برای مخاطبان خود - به‌ویژه اگر مخاطبانشان افرادی از فرهنگ‌های غیر باشند - تهدید به بار می‌آورند. آنها از طریق متقاعد کردن مخاطبان و ایجاد شرایط لازم برای پذیرش پیام‌های خود، به‌طور تدریجی هویت مخاطبان را آن گونه که خود می‌خواهند تغییر می‌دهند و با درونی کردن باورهای خود در ذهن مخاطبان رضایت آنها را نسبت به پذیرش هویت جدید و انکار هویت خود جلب می‌کنند.^(۱۲)

در شبکه‌های اجتماعی مجازی مانند همه انواع رسانه‌ها از نشانه‌های کلامی و غیرکلامی برای ایجاد ارتباط و ایجاد تغییر در باورها و ارزش‌ها استفاده می‌شود. از جمله نشانه‌های کلامی مورد استفاده در این رسانه‌ها عبارتند از:

۱. استفاده کردن از ارزش‌ها برای اعتبار بخشیدن به خود،
۲. وانمود کردن به همسویی با جمع،
۳. برچسب‌زنی و اسم‌گذاری،
۴. استفاده از آمار و ارقام،
۵. توسل به عواطف و احساسات مخاطبین،
۶. تحریف،
۷. مقایسه،
۸. شایعه،
۹. کلمات اثربخش و ...

همچنین نشانه‌های غیرکلامی مبهم عبارتند از:

۱. رنگ،



۲. موسیقی،
۳. تبلیغ در تبلیغ،
۴. تصاویر غیرقابل انتظار،
۵. طنز و کاریکاتور،
۶. تصاویر کلیشه‌ای،
۷. نشانه‌های بیانی،
۸. حرکات چهره،
۹. حرکات اندام و ...^(۱۲)

در شبکه‌های اجتماعی با توجه به شیوه کارکرد آنها و ابزارهای کلامی و غیرکلامی مورد استفاده در آنها، تعاملات اجتماعی بستری مناسب برای رشدی خارج از محدودیت و چارچوب‌های مرسوم می‌یابند. محدودیت‌ها و چارچوب‌هایی چون آداب و رسوم، عرف و عادات، قانون مکتوب و غیرمکتوب، شرع (دین و مذهب) و قدرت دولت در تعاملات اجتماعی غیرمجازی، دامنه این تعاملات را تعریف می‌کنند، ولی در تعاملاتی که در شبکه‌های اجتماعی مجازی صورت می‌گیرد نه تنها مرزهای سرزمینی، بلکه همه انواع مرزها از میان برداشته می‌شود.

کاستلز معتقد است از آنجا که انتقال و جریان فرهنگ از طریق ارتباطات صورت می‌گیرد، حوزه فرهنگ که نظامی از عقاید و رفتارها را شامل می‌شود با ظهور تکنولوژی جدید دستخوش دگرگونی‌های بنیادین می‌گردد. ورود فناوری‌های ارتباطی جدید، با تغییر ساختار مناسبات و ارتباطات انسانی منجر به شکل‌گیری نوع جدیدی از تعاملات انسانی شده است.^(۱۳)

ارتباطات و تعاملات مذکور راهگشای نگرستن به انسان به عنوان پدیده‌ای چند لایه، تغییرپذیر، منفعل و تکه‌تکه است. پدیده‌ای که شکل دادن خویش را به‌گونه‌ای طراحی می‌کند که با هرگونه تثبیت هویت می‌ستیزد. جامعه اطلاعاتی مبتنی بر فضای مجازی مشوق هویت بی‌ثبات، تغییرپذیر و منعطف انسان جدید است.^(۱۴) شری ترکل این موضوع را به این صورت توصیف کرده است: «ما بر روی اینترنت تشویق می‌شویم که به خودمان به صورتی سیال، بر آینده تمرکززدایی شده، چندگانه شده، انعطاف‌پذیر و همیشه درحال فرآیند فکر کنیم». بنابراین «اینترنت به آزمایشگاه اجتماعی مهمی برای تجربه کردن ساختن و بازساختن خویشتن بدل شده است که خصلت زندگی پست‌مدرن است».^(۱۵)

فضای مجازی این امکان را به فرد می‌دهد که مراجع و منابع مختلف و متعددی را در اختیار داشته باشد، منابع و مراجعی که هر کدام ارزش‌های خاص خود و سبک زندگی ویژه‌ای را ترویج می‌کنند. این درحالی است که تمامی مرزهای هویتی، مثل خانواده، محله، قومیت و ملیت به‌شدت نفوذپذیر شده‌اند. در دنیای به‌هم پیوسته عصر اطلاعات مرجعیت خانواده از بین رفته و در اثر

تنیدگی جهان هویت‌های منسجم و یگانه از دسترس جوانان و نوجوانان خارج شده و هویت آنها دچار چندپارگی و انشقاق شده است. لذا آنچه قابل مشاهده است نه فرآیند آرام و پیوسته انتقال هویت از نسلی به نسل دیگر، بلکه بحران‌های هویتی است.^(۱۶)

فضای مجازی و به‌ویژه شبکه‌های اجتماعی نه تنها با تغییر هویت‌های ملی کشورها، امنیت داخلی آنها را به خطر می‌اندازند، بلکه به‌طور مستقیم نیز باعث به خطر افتادن امنیت می‌شوند. بدون اینکه بخواهیم سودمندی و مزایای شبکه‌های اجتماعی به‌عنوان ابزارهایی که می‌توانند به مردم‌سالاری و شفافیت و در نتیجه کارآمدی نظام‌های سیاسی کمک کنند را کتمان کنیم، لازم است ظرفیت‌های بسیار بالای آنها را در ایجاد بحران‌های امنیتی نیز مورد توجه قرار دهیم. افراد یک جامعه با عضویت در شبکه‌های اجتماعی گذشته از اینکه وارد جامعه چند ده میلیونی و گاهی چند صد میلیونی در سطح جهان می‌شوند، در داخل کشور خودشان نیز مانند حزبی اجتماعی و سیاسی رفتار می‌کنند. رفتارهای سیاسی این حزب ثبت نشده و مسئولیت‌ناپذیر همیشه در جهت اعتلای مردم‌سالاری و پیشرفت امور نیست. این نیروی منسجم اجتماعی و سیاسی هر آن ممکن است با وقوع اتفاقی - بسته شدن روزنامه‌ای، اعدام مجرمی، بالا رفتن تورم، بالا رفتن نرخ بیکاری، انتخاب نشدن کاندیدایی برای تصدی پستی سیاسی و... - به انحای مختلف به اعتراض پرداخته و حتی اقدام به خرابکاری و سلب امنیت داخلی کند. نافرمانی این نیروی داخلی آن زمان به ایجاد بحران امنیتی منجر می‌شود که حادثه‌ای ازسوی منبعی، به صورت تحریف شده یا سوءتعبیر شده - عمداً یا سهواً - از طریق شبکه اجتماعی به اطلاع اعضا رسانده شود.

گزارش‌های کذب، تحریف شده و گزارش‌هایی که با برداشت‌ها و تفسیرهای شیطنت‌آمیز ارائه می‌شوند می‌توانند اعضای شبکه‌های اجتماعی را علیه رهبران سیاسی جامعه بشورانند. فهم این نکته چندان سخت نیست که در دنیایی که دشمنی و جنگ بُعد دیگری به نام جنگ نرم پیدا کرده است منابع متعددی در قالب دوست و عضو شبکه ممکن است اقدام به پراکندن شایعات متعدد کرده و آن دسته از شهروندان کشورها را که عضو شبکه‌های اجتماعی هستند به اقدام علیه رهبران سیاسی خود بسیج کرده یا آنها را نسبت به رهبران خود بدبین کنند و بدین ترتیب مشروعیت سیاسی آنها را با بحران مواجه کرده و امنیت داخلی را از کشورها سلب کنند.

همچنان که می‌دانیم واقعیت دولت‌ها با حاکمیت آنها بر همه امور در سرزمین خودشان تحقق می‌یابد. هر چند که امروزه دانشمندان از حاکمیت متکثر سخن گفته و از سهم بودن شرکت‌ها و بخش‌های دیگری در حاکمیت دفاع کرده‌اند، اما دانشمندان دیگری حاکمیت را جزء جدایی‌ناپذیر دولت دانسته‌اند. حتی دانشمندان طرفدار متکثر بودن حاکمیت نیز قبول دارند که حاکمیت باید در



دست دولت و گروه‌هایی که مسئولیت‌پذیر و پاسخگو هستند، باشد. با این توصیف مشکل اصلی دولت‌های امروز در رابطه با شبکه‌های اجتماعی حاکمیتی است که دولت‌ها از دست می‌دهند و شبکه‌های اجتماعی بدون هیچ نوع احساس مسئولیتی آن را به دست می‌آورند.

در این خصوص کاستلز معتقد است ارتباطات کامپیوتری از کنترل دولت‌های ملی می‌گریزد و این امر دولت‌ها را به هراس انداخته است. کاستلز می‌گوید در ژانویه ۱۹۹۶ وزیر تکنولوژی اطلاعات فرانسه قصد دولت خویش را مبنی بر پیشنهاد مجموعه روش‌هایی به اتحادیه اروپا برای محدود ساختن دسترسی آزاد به اینترنت اعلام کرد. او این واقعه را طرحی برای سانسور تکنولوژیک، آن هم از سوی کشوری که آرمان‌های انقلابی آزادی را در اروپا انتشار داده بود می‌نامد.^(۱۷) در دست داشتن حداکثر حاکمیت - به‌ویژه به‌منظور حفظ توان ایجاد نظم و امنیت در داخل - آرزوی همه کشورهاست. از جمله چین با عنوان برقراری توازن میان جریان آزاد اطلاعات و پاسداشت فرهنگ و ارزش‌های اجتماعی دست به اقدامات گسترده‌ای زده است. چین در این راستا اقدام به تأسیس شرکت دولتی اینترنت و انحصار ورود اینترنت به کشور از طریق این شرکت کرده است. این کشور همچنین هزینه‌های عظیمی را برای فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت متحمل شده است.^(۱۸) حتی آمریکا که خود را مدافع سرسخت آزادی اینترنت و دسترسی آسان به اینترنت در سراسر جهان می‌داند و این ژست را به خود می‌گیرد که نسبت به ظرفیت‌های اینترنت و قدرت ارتباط‌دهندگی آن و شبکه‌های اجتماعی مجازی آگاه بوده و آنها را تقویت می‌کند، هر جا که لازم باشد نسبت به کنترل، سانسور و حذف و قطع آن به بهانه دفاع از امنیت ملی و امنیت زندگی خصوصی اقدام می‌کند.^(۱۹)

در کل باید گفت فضای مجازی و به‌ویژه شبکه‌های اجتماعی از جنبه‌های مختلفی امنیت ملی را تحت تأثیر قرار می‌دهند که عبارتند از:

۱. موجبات کم‌رنگ شدن حاکمیت ملی دولت‌ها را فراهم می‌آورند،
۲. موجب بروز بی‌مرزی‌های فکری - فرهنگی می‌شوند،
۳. موجبات نزدیکی و تعامل هرچه بیشتر نهادهای فکری که علی‌القاعده خارج از کنترل دولت‌ها عمل می‌کنند را فراهم می‌آورند،
۴. موجب تغییر و تحول خواست‌های مردمی می‌شوند،
۵. موجب تغییر تصور مردم از کارآیی نظام سیاسی می‌شوند،
۶. ایدئولوژی تثبیت شده نظام سیاسی را با تغییر نگرش مردم به چالش می‌کشند،^(۲۰)
۷. با تغییر جهان‌بینی‌ها و عقاید مردم هویت آنها را متحول کرده و در نتیجه موجب سرگشتگی، بی‌هویتی، دنباله‌روی، غرب‌گرایی، فردیت و انزوای اجتماعی می‌شوند.

شبکه‌های اجتماعی در خدمت اهداف سیاسی آمریکا

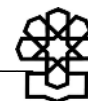
همان گونه که اختراع اینترنت و استفاده از آن به صورت گسترده از آمریکا شروع شد، اختراع شبکه‌های اجتماعی مثل فیس‌بوک و توییتر نیز - با گذشت چند دهه - در آمریکا رخ داد. اینترنت در بدو اختراع در خدمت مقاصد نظامی و سیاسی آمریکا بود، بنابراین دستگاه‌های نظامی، جاسوسی و سیاسی آمریکا کاملاً از ظرفیت‌های آن برای بهره‌برداری به‌منظور رسیدن به اهداف سیاسی و نظامی آگاه بودند. این بود که با افزایش عضویت کاربران اینترنت در شبکه‌های اجتماعی مقامات سیاسی و دفاعی و امنیتی این کشور درصدد مدیریت و کنترل آنها و درصدد استفاده از آنها برای تجسس، جمع‌آوری اطلاعات، نظرسنجی و... افتادند.

هر چند از چگونگی ارتباط شبکه‌های اجتماعی مشهوری مانند فیس‌بوک و توییتر با سازمان‌های نظامی، سیاسی و جاسوسی آمریکا اطلاعات زیادی در دست نیست و بیشتر اطلاعات مربوط به حدس و گمان‌های دانشمندان حوزه امنیت، فضای مجازی، روابط بین‌الملل و مطالعات منطقه‌ای است، با این حال شواهد آشکاری که دولت آمریکا هرگز آنها را کتمان نکرده است، نشان می‌دهند مقامات آمریکایی سعی دارند تا سیاست‌ها و اهداف امنیتی و دفاعی خود را به دست‌اندرکاران این شبکه‌ها دیکته کنند و آنها را به شیوه‌های مختلف با سیاست‌های خود همراه سازند. در این راستا دیک کستولو^۱ مدیرعامل توییتر در می سال جاری میلادی از سوی اوباما به‌عنوان عضو گروه مشاوران وی منصوب شد. همچنین مارک زاکربرگ مدیرعامل و بنیانگذار فیس‌بوک در اجلاس گروه ۸ در فرانسه شرکت و با مقامات این گروه دیدار کرد.^(۲۱) این امر بیانگر اهمیت این شبکه‌ها در تحقق اهداف دولت‌هاست.

اخیراً نیز مؤسس سایت ویکی‌لیکس، جولیان آسانژ، ادعا کرده است که فیس‌بوک عامل اطلاعاتی آمریکاست. جولیان آسانژ که با شبکه روسی راشاتودی مصاحبه می‌کرد مدعی شده است هر کسی که عضو این شبکه اجتماعی می‌شود به‌طور غیرمستقیم با عوامل اطلاعاتی آمریکا همکاری می‌کند.

کارشناسان امور آی‌تی ادعای آسانژ را تأیید کرده‌اند از جمله جان سی دورک می‌گوید: در عصر حاضر قدرت‌های بزرگ از هر ابزاری برای جاسوسی استفاده می‌کنند و درحال حاضر اینترنت و فضای مجازی بهترین ابزاری است که آنها در اختیار دارند. او با تأکید بر این موضوع که ادعای آسانژ را نمی‌توان رد کرد، اظهار می‌کند عضویت در سایت‌هایی چون فیس‌بوک، توییتر، فلیکر و... برای کاربران خطرناک است. برای برخی از کاربران قرار دادن اطلاعات شخصی‌شان در

1. Disk Costolo



صفحه خود موضوع مهمی نیست، اما در آینده برای آنها پیامدهای جدی در پی دارد. او بدون هیچ شکی تأکید می‌کند قدرت‌های جهان در عصر حاضر از طریق فیس‌بوک از افراد جاسوسی می‌کنند.^(۲۲) به گفته کارشناسان به دنبال شهرت جهانی فیس‌بوک سازمان سیا برای تحت کنترل گرفتن این سایت با هدف استفاده از اطلاعات شخصی کاربران مدتهاست که وارد عمل شده است. فیس‌بوک دقیقاً سیاست‌های قدرت‌های بزرگ را اعمال می‌کند که به دنبال افزایش قدرت و نفوذ خود در جهان هستند. قطعاً سازمان سیا از طریق فیس‌بوک می‌تواند عوامل زیادی برای انجام جاسوسی در کشورهای مختلف به خدمت گیرد.^(۲۳)

آمریکا همچنین به استفاده از شبکه‌های اجتماعی مجازی با عنوان «دیپلماسی دیجیتال» و در واقع به منظور ارتباط با مردم کشورهای دیگر روی آورده است. در این دیپلماسی جدید که سیاست خارجی آمریکا توسط جارد کوهن و الک راس از مشاورین وزارت امور خارجه آمریکا طراحی و مدیریت می‌شود دو مشاور مذکور اقدام به ارسال پیام‌های بی‌شماری در توییتر می‌کنند. پیام‌هایی که این دو ارسال می‌کنند ترکیبی از دیپلماسی و زبان عامیانه است و در این شبکه شهرت بسیاری یافته‌اند. هیلاری کلینتون، وزیر امور خارجه آمریکا، در شکل‌گیری و توسعه این نوع از دیپلماسی نقش فعالی دارد به نحوی که وی را «مادرخوانده دیپلماسی دیجیتال آمریکا» می‌نامند. در این نوع دیپلماسی نیز باز مقامات آمریکایی درصدد جلب همکاری مدیران سایت‌ها و شبکه‌های فضای مجازی هستند. به‌عنوان مثال کوهن و راس با حمایت وزارت امور خارجه آمریکا ضیافت شامی خصوصی با حضور وزیر امور خارجه ترتیب دادند و از ۱۰ شخصیت مهم در عرصه تکنولوژی ارتباطی و رسانه‌های اجتماعی از جمله مدیر ارشد اجرایی گوگل و بنیانگذار و رئیس توییتر خواستند که در این مهمانی حضور داشته باشند. در این ضیافت شام وزیر امور خارجه آمریکا با اشاره به اولویت رسانه‌های دیجیتال در سیاست خارجی این کشور از این ۱۰ شخصیت خواست تا با دولت آمریکا در زمینه پیشبرد و توسعه دیپلماسی همکاری کنند.^(۲۴)

این البته نوع جدیدی از دیپلماسی آمریکایی نیست، بلکه عنوان دیگری بر نحوه جدید دخالت آنها در امور داخلی کشورهای دیگر است. آمریکایی‌ها در تکمیل این نوع خاص از سیاست خارجی خود پول‌های زیادی را برای مبارزه با فیلترینگ شبکه‌های اجتماعی در کشورهای توسعه‌نیافته هزینه می‌کنند. دن‌بائر دستیار معاون وزارت امور خارجه آمریکا در امور دموکراسی و حقوق بشر در مصاحبه‌ای به شبکه خبری بلومبرگ گفته است قرار است یک برنامه ۵۰ میلیون دلاری برای کمک به اپوزیسیون‌های فعال در اینترنت اجرا شود. این برنامه به تولید نرم‌افزارهایی کمک خواهد کرد که در ایران و سوریه استفاده شوند و هدف آن کمک به مخالفان فعال برای جلوگیری از شناسایی شدن است. وزارت خارجه گروهی از مخالفان را با توانایی‌های فنی تشکیل داده است تا

به جنبش‌های معترض در کشورهای مثل ایران و چین کمک کند. به گفته او این گروه چگونگی پرهیز از شناسایی شدن هنگام استفاده از سرویس‌هایی مثل توییتر را به بیش از پنج هزار نفر آموزش داده است. همچنین وزیر خارجه آمریکا گفته است آمریکا با ارائه تکنولوژی‌های غلبه بر فیلترینگ به مخالفینی که در محیط‌های محدود اینترنتی هستند، کمک خواهد کرد.^(۲۵)

البته آمریکا برای فشار آوردن بر دولت‌هایی که با سیاست‌های آمریکا همسو نیستند رأساً نیز برای دخالت در امور داخلی آنها به ایجاد شبکه‌های اجتماعی اقدام می‌کند. شبکه صدای آمریکا (VOA) با همکاری شرکت شهروند جهانی^۱ قصد دارد تا سرویسی راه‌اندازی کند که با آن فیلترهای آنلاین کشورهای دیگر را از بین ببرد و همچنین مخاطبانش هر نوع مطلبی را که می‌خواهند به صورت متن، فیلم و یا عکس بر روی آن بارگذاری کنند تا شبکه VOA مهمترین خبرها را در اختیار گزارشگران قرار دهد. والتر ایزاکسن مدیر سابق CNN و مدیر فعلی شورای پخش برنامه آمریکا (BBG) گفته است سازمان‌های خبری دولتی، مانند VOA یا رادیو آسیای آزاد در صورت ممکن از رسانه‌های اجتماعی استفاده خواهند کرد. وبسایت کانتر پانچ که خبر مذکور را نقل کرده، بر این نظر است که استفاده از رسانه‌های اجتماعی از سوی سرویس‌های خبری دولتی آمریکا در جهت از بین بردن فیلترهای آنلاین کشورهای دیگر صورت می‌گیرد.^(۲۶)

کاربرد دیگر شبکه‌های اجتماعی برای مقامات آمریکا، استفاده از امکانات آن برای ایجاد ارتباط با مردم جهان به منظور توجیه سیاست‌های خارجی آمریکاست. این کار در واقع قسمت دیگری از «دیپلماسی دیجیتال» آمریکاست، با این تفاوت که در قسمت قبلی هدف از به‌کارگیری آن، متقاعد کردن مردم سرزمین‌های خارجی برای اعتراض و قیام علیه دولت‌های داخلی خودشان بوده، ولی در این قسمت، آمریکا با استفاده از شبکه‌های اجتماعی سیاست‌های خارجی مداخله‌جویانه، استعمارگرانه، جنگ‌افروزانه و تروریستی خود را در پس الفاظ پرطمطراقی چون حفظ نظم و ثبات، کمک به پیشرفت و ترقی و مبارزه با تروریسم، توجیه می‌کند. روزنامه آمریکایی هافینگتون پست گزارش می‌دهد که در اداره اصلی فرماندهی مرکزی آمریکا (سنتکام) در شهر تامپای ایالت فلوریدا، تیمی با نام «مبارزه دیجیتال» تشکیل شده است و اعضای آن مشغول مقابله با پیام‌های افراطی هستند که در وبلاگ‌ها و محیط‌های گفتگوی اینترنتی مطرح می‌شود. اعضای این تیم که مسلط به زبان‌های عربی، فارسی و اردو هستند در دنیای مجازی به دنبال اظهارات نادرست یا به‌زعم آنها آتش‌افروز درباره عملیات یا فعالیت‌های ارتش آمریکا هستند. زمانی که اعضای این تیم این پیام‌ها را پیدا می‌کنند خود را برای تعامل با این نوشته و به چالش کشیدن حقایق یا منطق نویسنده پیام آماده می‌کنند.^(۲۷)



وزارت امور خارجه رژيم صهيونيستي اسرئيل نيز تيمي را براي فعاليت در فضاي مجازي اينترنت با هدف بهبود تصوير اين رژيم ايجاد کرده است. يکي از اقدامات اين گروه نوشتن مطالب مختلف در سايت‌هاي فيس‌بوک و توييتر در ۲۴ ساعت شبانه‌روز است. اعضاي اين گروه در فضاي مجازي خود را کاربران عادي معرفي مي‌کنند و از فاش کردن هويت اسرئيلي خود پرهيز مي‌کنند. البته اين گروه زيرمجموعه بخش بزرگ‌تري تحت عنوان «هسبار» به معني «توضيح مردمی» در وزارت خارجه اسرئيل است. اين گروه با مسئوليت فردي به نام «ايلان شتورمان» فعاليت مي‌کند. شتورمان مي‌گويد اين گروه به‌طور سري کار مي‌کند. آنها نظرات خود را در سايت‌هاي مختلف مي‌نويسند و به ديگر نظرات پاسخ مي‌دهند و طوري وانمود مي‌کنند که کاربر عادي اينترنت هستند. اين تيم در سايت‌هاي مختلف از جمله تالارهاي گفتگو، وبلاگ‌ها، توييتر و فيس‌بوک فعال هستند. اين تيم سعي مي‌کند با تماس با يهوديان در سراسر جهان، آنها را به نوشتن مطلب به زبان کشور محل اقامت خود در اينترنت و توضيح دادن مواضع اسرئيل ترغيب کند. همچنين هنگامي که مقاله‌اي انتقادآمیز از اسرئيل در فضاي اينترنت منتشر مي‌شود، آنها تلاش براي پاسخ و واکنش به اين مقاله را آغاز مي‌کنند. اين تيم، همچنين مطلبي را عليه گروه‌ها و اشخاصي که از فلسطيني‌ها دفاع مي‌کنند، منتشر مي‌کنند.^(۲۸) البته صرف استفاده از شبکه‌هاي مجازي و ساير امکانات فضاي مجازي براي توضيح مواضع و نشان دادن تصويري مطلوب از کشور، به منزله سوءاستفاده از امکانات فضاي مجازي نيست. آنچه در اين موضوع قابل توجه است، استفاده از اينترنت براي توجيه تجاوز و تروريسم دولتي است که آمريکا و رژيم غاصب اسرئيل به راه انداخته‌اند. بي‌شک اين موضوع ارتباط مستقيمي با امنيت داخلي کشورهايي دارد که با سياست‌هاي تجاوزگرانه اين دولت‌ها مخالفند. زيرا آنها مي‌توانند شهروندان داخلي کشورهاي مخالف را به ناحق مجاب کنند که حملات و اقدامات تجاوزکارانه و تروريستي‌شان مثلاً دفاع مشروع، حفظ نظم، جلوگيري از تروريسم و ... محسوب مي‌شود و دولت‌هاي آنها دشمني ناعادلانه و غيرمنطقي‌اي را دنبال مي‌کنند.

ستاد مشترک ارتش آمريکا نيز از استفاده از تکنولوژي‌هاي ارتباطي جديد غافل نمانده و در آوريل ۲۰۰۹ با ايجاد يک اکانت توييتر براي درياسالار مايک مولن، رئيس ستاد، خود را وارد جهان رسانه‌هاي اجتماعي کرده است. رئيس ستاد مشترک از وبسایت‌هاي رسانه‌هاي اجتماعي براي انتشار اطلاعات و نيز جمع‌آوری نظرات بيان شده در مورد اطلاعات منتشر شده استفاده مي‌کند. بدین ترتيب او مي‌تواند تأثيرگذاري پيام‌ها را سنجيده و مسائل رايج در افکار عمومي را شناسايي کند.^(۲۹)

شبکه‌های اجتماعی و امنیت ملی جمهوری اسلامی

اخذ و استفاده از تکنولوژی‌های ارتباطی و نیز بهبود و اصلاح کارکردهای انواع تکنولوژی‌های ارتباطی همواره مورد توجه ایرانیان بوده است. با ورود جهان به عصر اطلاعات و ارتباطات دیجیتال ایران نیز سعی کرد تا از آخرین پیشرفت‌های بشری در قلمرو فضای مجازی استفاده کند و تا حد امکان برای ابداع روش‌ها و وسایل جدید دیجیتالی تلاش نماید.

با شروع نقطه عطف دیگری در ارتباطات مجازی - ابداع وبلاگ‌ها و شبکه‌های اجتماعی مانند یوتیوب، توئیتر، فیس‌بوک و ... ایرانیان نیز به استفاده از این تکنولوژی‌ها روی آوردند به طوری که در سال‌های ۱۳۸۳ و ۱۳۸۴ رتبه چهارم و بنویسی جهان را به دست آوردند. ایرانی‌ها همچنین در سال‌های ۱۳۸۴ تا ۱۳۸۵ رتبه سوم در میان اعضای «اورکات» را از آن خود کرده بودند. این رقم البته از آمار رسمی این پایگاه به دست می‌آید و شامل ایرانیانی که محل اقامت خود را خارج از کشور ذکر کرده‌اند، نمی‌شود. برخی پایگاه‌های مشابه نیز نوعی شبکه اجتماعی مجازی ایرانی به شمار می‌روند که ۱۰۰ درصد کاربران آنها از ایران هستند.^(۳۰)

مهمترین دلایل عضویت و استفاده ایرانیان از شبکه‌هایی مثل فیس‌بوک چهار دلیل عمده است:

۱. کسب اطلاعات و اخبار،

۲. دوست‌یابی و ارتباط،

۳. سرگرمی،

۴. قابلیت‌های شبکه‌سازی.

برای اغلب کاربران اینترنت در ایران شبکه‌های اجتماعی مجازی ضمن داشتن قابلیت دوست‌یابی، کارکرد کسب اطلاعات و اخبار را دارد. برای نزدیک به ۴۰ درصد از کاربران ایرانی شبکه‌های اجتماعی، کارکرد کسب اطلاعات و اخبار این شبکه‌ها مهمترین دلیل آنها برای مراجعه به این شبکه‌هاست. به عبارت دیگر، به دلیل قابلیت به اشتراک‌گذاری و انتشار سریع اطلاعات و اخبار در محیط این شبکه‌ها، بسیاری از کاربران از طریق این محیط‌های مجازی به کسب اطلاعات و خبرهای روز ایران و جهان می‌پردازند. در بین شبکه‌های اجتماعی، فیس‌بوک بیشترین تعداد کاربران ایرانی را به خود اختصاص داده است.^(۳۱)

اهمیت خاص اینترنت، تعامل گروه‌های مرجع با آن است. به علت محدودیت نسبی دسترسی به اینترنت، کسانی که به اینترنت دسترسی دارند از نوعی مرجعیت برخوردارند و کلام بازگفته از این پایگاه اینترنتی از نوعی ارجحیت بی‌چون و چرا برخوردار می‌شود. شاید این همان باشد که رئیس آژانس فدرال ارتباطات و اطلاعات دولتی (FARST) در روسیه آن را «هجوم ارتباطات نوین به



روان‌شناسی افراد و ملت‌ها» نامیده است.^(۳۲)

ناممکن بودن پنهان نگه داشتن اسرار، نبود امکان کنترل داده‌های تبادل شده در شبکه‌های ملی و جهانی، دسترسی‌های غیرمجاز به شبکه‌های امنیتی و شکست امنیت شبکه‌های ملی، خصوصاً در بخش اقتصادی و بانکی و جاسوسی رایانه‌ای از مواردی جدی است که آسیب‌پذیری امنیت ملی را در مقابل فناوری ارتباطی و اطلاعاتی نمایان می‌کند. تضعیف شدید زبان و به‌خصوص خط ملی از دیگر جنبه‌های مهم در تضعیف امنیت ملی است.

همچنین از طریق آگهی‌هایی که شکل و صورت معتبر دارند ممکن است افرادی در تخصص‌های مختلف و حتی به‌صورت کارگران ماهر یا ساده دعوت به همکاری شوند، اما در عمل بدون اینکه هیچ نوع شغلی به دست آورند مورد انواع سوءاستفاده‌ها و کلاهبرداری‌ها قرار گیرند.

از نظر امنیت سیاسی، کافی است به موتورهای جستجو مراجعه کرده و واژه ایران را در یکی از آنها جستجو کنیم، تعداد صفحاتی که از طریق این موتورهای جستجو - گوگل، آلتاوسیتا، ام اس ان، یاهو و ... - پیدا می‌شود در مواردی بالغ بر یک میلیون صفحه است. با توجه به طبقه‌بندی فیشر از تهدیدات امنیت ملی، برخی از این صفحات می‌تواند موجب تقویت منابع خارجی تهدیدات از جمله تبلیغات منفی علیه حکومت باشد. درحال حاضر تبلیغات سیاسی شدیدی در اینترنت علیه ایران انجام می‌گیرد. با مراجعه‌ای گذرا به یک صفحه وب مانند www.gooya.com می‌توان به نشانی اینترنتی چندین گروه مخالف تا برانداز نظام، سازمان‌های قوم‌مدار، نشریات ضدحکومت و چندین انجمن تبلیغات دینی غیراسلامی دسترسی داشت. برخی از این گروه‌ها فقط حیات اینترنتی دارند و صرفاً با استفاده از اینترنت و بدون هیچ فعالیت عملی یا عملیاتی به انتشار دیدگاه‌های سیاسی و اخبار می‌پردازند و حتی گروه‌های غیرفعالی مانند فرقان و آرمان مستضعفان جزوهای عقیدتی، بیانیه‌ها و گزارش‌های عملیات‌های خود در سال‌های ۱۳۵۲-۱۳۵۵ را بر روی اینترنت قرار داده‌اند. برخی از این گروه‌ها مانند منافقین از طریق اینترنت نسبت به جمع‌آوری اخبار، جذب هواداران و آموزش عملیات خرابکارانه مبادرت می‌کنند.^(۳۳)

جنگ نرم دولت‌های غربی و در رأس آنها آمریکا علیه ایران چیزی نیست که بتوان وجودش را انکار کرد. دولت‌های غربی پس از شکست‌هایشان در فشارهای نظامی و اقتصادی بر ایران به فکر راه‌اندازی جنگ نرم علیه نظام جمهوری اسلامی افتادند. از جنبه‌های مهم و اصلی جنگ نرم آمریکا و متحدانش علیه ایران استفاده از اینترنت و به‌ویژه شبکه‌های اجتماعی برای شایعه‌پراکنی، اختلاف‌افکنی، ایجاد تغییر در باورها و اصول در ایران است. آمریکا در این راستا ۵۰ میلیون دلار - به‌عنوان بخشی از بودجه ۵۰۰ میلیارد دلاری وزارت دفاع - برای نفوذ در ایران، مقابله با فیلترینگ سایت‌های ضد ایرانی، تحریک قربانیان سانسور در ایران، آموزش الکترونیکی ایرانیان مخالف نظام

برای براندازی نرم و شبکه‌سازی اینترنتی برای اغتشاشگران بعد از انتخابات ریاست‌جمهوری و ارائه آموزش‌های لازم رسانه‌ای و کامپیوتری برای راه‌اندازی سایت اختصاص داده است.^(۳۴)

آمریکا برای عملی کردن چنین اهدافی کنفرانسی را در واشنگتن با حمایت شرکت‌های بلندپایه نظامی خود برگزار کرد و متخصصان فناوری و نظامی را با هدف آموزش نیروهای ارتش و اطلاعات گردهم آورد تا به آنها بیاموزد که چگونه از اینترنت و سایر نرم‌افزارها در جنگ سایبر علیه ایران استفاده کنند. کریستوفر جی. پتریک، روزنامه‌نگار و ناشر آمریکایی که خود یکی از حاضران این نشست بوده است، طی گزارشی در هفته‌نامه «امریکن فری پرس» می‌نویسد: در کنفرانس اخیری که از سوی شرکت «بنیاد عملیات‌های اطلاعاتی» و با حمایت مالی «نورتروپ گرومن»، «جنرال داینامیکز»، «سایک»^۱ و برخی دیگر از شرکت‌ها برگزار شد، چگونگی فعالیت نیروها برای مداخله در ایران به دقت مورد بررسی قرار گرفت. پتریک ادامه داد: در این کنفرانس صدها نظامی کهنه‌کار، سرباز و روزنامه‌نگار، ۱۵۰ افسر نظامی ارتش آمریکا و تعداد بسیار زیادی از تجار آمریکایی حضور داشتند. سخنرانان نیز به‌طور دقیق چگونگی استفاده از نرم‌افزارها و سایت‌های اینترنتی را برای کمک به گروه‌های مخالف موسوم به اپوزیسیون ایران که خواستار براندازی دولت ایران هستند، آموزش دادند.^(۳۵)

مؤسسه «مطالعات خاور نزدیک واشنگتن» نیز اخیراً گزارشی را با موضوع استفاده از اهرم‌های اطلاعاتی برای فشار به ایران منتشر کرده است. مایکل آیزنشتات کارشناس ارشد و مدیر مؤسسه «مطالعات نظامی و امنیتی واشنگتن»، در این گزارش ضمن انتقاد از استراتژی دولت آمریکا در رویارویی با ایران خواستار راه‌اندازی برنامه‌ای استراتژیک برای قدرتمندسازی نیروهای مخالف داخلی در ایران و ایجاد شکاف در جمهوری اسلامی شده است تا بدین وسیله ایران به سمتی هدایت شود که برای کاهش فشار خارجی که به‌صورت داخلی نمود پیدا کرده از اهداف استراتژیک خود - مانند برنامه هسته‌ای و غنی‌سازی خود - صرف‌نظر کند.^(۳۶)

این گزارش ضمن تأکید بر نقش تعیین‌کننده قدرت نرم، از جمله موانع موجود در یک مبارزه اطلاعاتی مؤثر را استفاده از شیوه‌های قدیمی و منسوخ می‌نامند. آیزنشتات برای از میان برداشتن این مانع می‌نویسد: رادیو فردا و تلویزیون فارسی صدای آمریکا (VOA) دارای استانداردهای حرفه‌ای پایینی هستند، از تکنیک‌های قدیمی و منسوخ استفاده می‌کنند و معمولاً در مورد اخبار فوری واکنش‌کننده نشان می‌دهند. با توجه به این مسائل دولت آمریکا باید تمام توان خود را به‌کار گیرد تا با مردم ایران ارتباط برقرار کرده و مطمئن شود که آنها به اخبار سروقت و دقیق دست



می‌یابند. به‌منظور برطرف شدن این مسئله و آشننگتن باید به مقامات رسمی ابلاغ کند که علاوه بر رادیو فردا و صدای آمریکا به‌طور مداوم با دیگر شبکه‌ها برای مثال بی‌بی‌سی فارسی و وبلاگ‌های فارسی که نزد عامه ایرانیان از محبوبیت برخوردارند مصاحبه کنند.^(۳۷)

البته گزارش‌ها و راهکارهای آمریکایی برای دخالت در ایران و براندازی نرم از یک یا دو مؤسسه سرچشمه نمی‌گیرد، بلکه مؤسسات متعددی که از بودجه دولتی و در پاره‌ای موارد خصوصی استفاده می‌کنند درگیر در جنگ نرم علیه ایران هستند. برای مثال مؤسسه تحقیقاتی هریتیج ضمن گزارشی نقش شبکه‌های اجتماعی را در حوادث پس از انتخابات ۱۳۸۸ مورد تأکید قرار می‌دهد. گزارش مذکور خبرنگاری خیابانی را عامل مهم شروع مخالفت‌ها و اعتراضات مردمی پس از اعلام نتایج انتخابات می‌داند و می‌افزاید خبرنگاران خیابانی، گزارش‌ها، تصاویر، فیلم‌ها و اطلاعات خود را به سایت‌های خبری مشهور می‌فرستند تا به‌صورت حرفه‌ای ویرایش و تدوین شوند گاهی نیز خبرنگاری در شکل خبرنگاری شهروندی بروز می‌کند که در آن مضامین خبری ازسوی پدیدآوردگان در وب سایت‌های شخصی ارائه می‌شوند. به گزارش مدیا ویک از ۱۳ تا ۱۷ ژوئن (۲۳ تا ۲۷ خردادماه ۱۳۸۸) سایت Ireport.com (که توسط سی.ان.ان اداره می‌شود، اما در بالای سایت این مسئله تکذیب شده است)، ۱۶۰۰ گزارش از شهروندان ایرانی دریافت کرده است؛ در این مدت ۳ هزار نفر دیگر هم عضو این سایت شده‌اند.^(۳۸)

همچنین آمریکا برای ایجاد اختلاف در ایران صفحه فارسی توئیتر را ایجاد کرده است. الک راس، مشاور وزیر امور خارجه آمریکا در پاسخ به این سؤال که وزارت خارجه آمریکا چرا اقدام به راه‌اندازی توئیتر فارسی کرده است؟ گفت: دلیلش خیلی ساده است. صفحه فارسی توئیتر گزینه دیگری است برای ارتباط با مردم. هر چند فکر نمی‌کنم که معجزه کند، ولی ابزاری است که می‌تواند برای خبررسانی مورد استفاده قرار گیرد.^(۳۹)

عملکرد رسانه‌های آمریکا در حوادث سال ۱۳۸۸ به قدری شدید بود که دستیار وزیر خزانهداری آمریکا در زمان ریگان در این خصوص گفت: شاید مردم آمریکا هرگز متوجه نشوند که آیا انتخاباتی که اخیراً در ایران برگزار شد صحت داشت یا آنکه تقلبی در آن صورت گرفته بود. رسانه‌های آمریکا به عنوان ابزار تبلیغاتی عمل می‌کنند نه ابزار انتقال حقیقت. همچنین محمدحسین هیکل نویسنده مصری گفت: پیش از برگزاری انتخابات ایران هزاران سایت اینترنتی تأسیس شد که صاحبان آن تلاش می‌کردند مردم را سردرگم کرده و آنها را برای اعتراض به نتایج انتخابات تحریک کنند. بسیاری از این پایگاه‌های اینترنتی توسط اسرائیل راه‌اندازی شده بود.^(۴۰)

نقش اینترنت در حوادث سال ۱۳۸۸ به اندازه‌ای بود که دادستان تهران در مقدمه کیفرخواست متهمین گفت: در اغتشاشات اخیر به وضوح دیده شد از اینترنت به عنوان ابزاری فراگیر و کارآمد

در برگزاری جمععات غیرقانونی، اطلاع‌رسانی دروغین و فضاسازی اغواگرانه بهره‌برداری شد. آنچه در جریان انتخابات و پس از آن اتفاق افتاد سلسله‌اعمالی بود که به دنبال هم طرح‌ریزی و اجرا شد.^(۴۱)

سرمایه‌گذاری دشمنان ایران بر روی رسانه‌های فضای مجازی و شبکه‌های اجتماعی مجازی که نمونه آن را در حوادث سال ۱۳۸۸ مشاهده می‌کنیم، نشان می‌دهد که تأثیر رسانه‌های فضای مجازی بر امنیت داخلی تا چه اندازه می‌تواند زیاد باشد.

آسیب و تهدید شبکه‌های اجتماعی مجازی بر امنیت جمهوری اسلامی ایران را می‌توان در چند مورد خلاصه کرد:

۱. **اشاعه فرهنگ غربی:** شبکه‌های اجتماعی مجازی گذشته از اینکه محل خوبی برای تبلیغ کالاهای فرهنگی و کالاهای غیرفرهنگی مرتبط با فرهنگ مانند لباس و وسایل آرایشی و بهداشتی هستند مستقیماً نیز پیام‌ها و نمادهای فرهنگی غرب را به اشتراک گذاشته و ارزش‌های فرهنگی غرب را با جذابیت‌های خاصی که در تصاویر - عکس‌ها و فیلم‌ها - نوشته‌ها و اصوات (موسیقی، آواز و گفته‌های توصیفی و تحلیلی) وجود دارد، اشاعه می‌دهند.

۲. **تغییر و بحران هویت:** نفوذ سریع و گسترده شبکه‌های اجتماعی در کنار بسته بودن فضای فرهنگی کشور سبب شده تا تغییر هویت در میان کاربران ایرانی، به‌ویژه جوانان، بسیار زودتر حادث شود. این شبکه‌ها وضعیت جدیدی را به‌وجود آورده‌اند که باعث تغییر الگوی مصرف در تعدادی از جوانان شده است. رنگ باختن هویت ایرانی و تبدیل آن به هویت غربی تهدیدی است که باعث به‌وجود آمدن شکاف‌های اجتماعی و فرهنگی و در نهایت بحران هویت خواهد شد.^(۴۲)

۳. **اطلاع‌رسانی غیرقابل کنترل:** اطلاعاتی که از طریق شبکه‌های اجتماعی مجازی از یک منبع منتشر می‌شود در کمتر از چند دقیقه به‌طور شبکه‌ای و صعودی در کل شبکه و از آنجا که اعضای یک شبکه ممکن است در شبکه‌های دیگر نیز عضو باشند در سایر شبکه‌ها و در نتیجه در کل جهان پراکنده می‌شود. این نوع اطلاع‌رسانی غیرقابل کنترل از سوی دولت‌هاست و هیچ مانعی شیوع اطلاعات را در این شبکه‌ها محدود نمی‌کند. هرچند که مزایای این نوع اطلاع‌رسانی در مواردی مثل شیوع بیماری، وقوع حوادث غیرمترقبه و غیره انکارناپذیر است در مواردی مثل شایعه‌سازی برای ایجاد رعب و وحشت، برهم زدن تعادل اقتصادی، هتک حرمت افراد و غیره تبعات زیانبار و برگشت‌ناپذیری دارد. غیرقابل کنترل بودن اطلاعات همچنین امکان افشای اطلاعات سری و طبقه‌بندی شده نظامی و سیاسی و نیز به چالش کشیده شدن باورهای دینی و اصول اخلاقی را تشدید می‌کند.

۴. **رواج فردگرایی و انزوای طلبی:** شبکه‌های اجتماعی مجازی موجب رشد فردگرایی و



انزواطلبی افراد می‌شود. انسان‌هایی که بیشتر وقت خود را برای تعامل در فضای مجازی صرف می‌کنند گذشته از اینکه امکان تعامل رودررو با افراد جامعه و به‌ویژه اعضای خانواده را به لحاظ زمان از دست می‌دهند، چه‌بسا شخصیت فردمحوری پیدا می‌کنند و از تعاملات رودررو گریزانند و حتی در صورت قرار گرفتن در موقعیت‌های چهره به چهره، چه‌بسا روابط شکننده‌ای را با دیگران داشته باشند. فردگرایی بیش از حد و در لاک خود بودن تبعات اجتماعی و اخلاقی زیادی بر خانواده و جامعه تحمیل می‌کند.

۵. **ظهور انسان‌هایی با تابعیت بین‌المللی:** شبکه‌های اجتماعی مجازی به‌ظهور تابعیت بین‌المللی و انسان‌هایی که تعلق خاطری به سرزمین خاصی ندارند کمک می‌کند. کاهش وفاداری‌های ملی و روحیه وطن‌دوستی باعث تولید افکار و گرایش‌های جدایی‌طلبانه و گسترش مرکز‌گریزی سیاسی شده و آسیب‌های سیاسی و امنیتی جدی در پی خواهد داشت.^(۴۳)

۶. **تجهیز گروه‌های مخالف داخلی:** از دیگر آسیب‌های شبکه‌های اجتماعی مجازی بر امنیت داخلی، توانایی این شبکه‌ها در مخالف‌سازی افراد با نظام‌های مستقر و گردآوری مخالفان و سازماندهی آنها برای به راه انداختن حرکت‌های اعتراضی به انحای مختلف است. دشمنان نظام با استفاده از این شبکه‌ها می‌توانند با دستاویز قرار دادن مسائل اقتصادی، اجتماعی و ... مخالفانی را در یک محیط مجازی گردآورده و با اشارت‌های صریح و غالباً ضمنی ناآرامی‌هایی را در داخل مدیریت کرده و امنیت داخلی را به خطر بیندازند.

۷. **جاسوسی از شهروندان:** گرفتن اطلاعات مورد نیاز از شهروندان توسط سرویس‌های امنیتی بیگانه نیز یکی از آسیب‌های جدی شبکه‌های اجتماعی است که ممکن است افراد آگاهانه و ناآگاهانه در دام این شبکه‌ها بیافتند.

نتیجه‌گیری

امکانات جدیدی که در سایه تکنولوژی‌های ارتباطی مجازی جدید برای بشر امروزی ایجاد شده است، چالش‌های فراوان و شدیدی را بر امنیت داخلی کشورها به‌ویژه کشور ما ایران اعمال می‌کند. از جمله این چالش‌ها می‌توان بر امکان ایجاد و گسترش شکاف میان مردم و دین؛ عرفی کردن فضای اجتماعی و سیاسی؛ ترویج پاره‌ای از ارزش‌ها و مفاهیم غربی مغایر با ارزش‌های اسلامی؛ ترویج فرهنگ تهمت، افترا، دروغ‌پردازی و حیثیت‌زدایی، الگوسازی‌های کاذب و غیرارزشی،^(۴۴) اطلاع‌رسانی غیرقابل کنترل و امکان جاسوسی، ظهور انسان‌هایی با تابعیت بین‌المللی، تضعیف زبان، رواج فردگرایی و انزواطلبی^(۴۵) اشاره کرد.

با این حال، چاره‌ای جز اذعان بر این موضوع نداریم که امکان جلوگیری از پیشرفت و توسعه تکنولوژی در هیچ جامعه‌ای وجود ندارد. شبکه‌های اجتماعی و فضای مجازی در کل از دست محدودکننده دولت‌ها می‌گریزند. در عین حال اعمال سانسور و تحدید آنها جامعه را از مزایای فراوانی که می‌توانند بر جامعه داشته باشند محروم می‌کند. دولت‌ها از این تکنولوژی‌ها می‌توانند برای اطلاع‌رسانی به موقع در مواقع بحران‌های طبیعی و غیره، کمرنگ کردن تعصبات قومی و تقویت انسجام و یکپارچگی ملی؛ آموزش و تعلیم و تربیت آنلاین و کم هزینه، آشنایی افراد با تنوعات زبانی، قومی و فرهنگی در داخل، یادگیری از جنبه‌های مثبت فرهنگ‌های قومی و استفاده از آنها برای ابتکارات و اختراعات ملی و غیره استفاده کنند. در عین حال آسیب‌های این شبکه‌ها نیز برای امنیت ملی جدی است.

اما برای مصون ماندن از خطرات شبکه‌های اجتماعی و فضای مجازی و یا حداقل کاستن از خطرات آنها راهکارهای زیر تا حدودی می‌توانند مفید باشند:

۱. رصد شبکه‌های اجتماعی و فضای مجازی برای کشف هویت‌های جعلی و مشکوک و آگاهی از شیوه‌های جاسوسی: شایسته است که گروهی به‌عنوان گروه پدافند عملیات‌های مجازی تشکیل شود تا به‌طور مداوم اینترنت و به‌ویژه شبکه‌های اجتماعی را مورد رصد قرار داده و ضمن کشف هویت‌های جعلی و مشکوک، موضوعات مطرح شده از سوی آنان و شیوه‌های آنان برای سوءاستفاده از مسائل مطرح شده را تحلیل و تجزیه کرده و با رعایت جوانب احتیاط با کاربران ایرانی وارد تعامل شوند و آنها را با شیوه‌های اقناع‌کننده روان‌شناسانه در جریان اصل موضوع قرار داده و نسبت به شیطنت‌های خصمانه آگاه کنند.

۲. ورود جدی و فعالانه به شبکه‌های اجتماعی و فضای مجازی برای تعامل با کاربران و اعضای ایرانی و خارجی شبکه‌ها و هدایت آنها: لازم است که تیم دیگری با برنامه و چشم‌اندازی طراحی شده در شبکه‌های اجتماعی فعالانه حضور داشته باشد تا با استفاده از شیوه‌های ظریف و ماهرانه تعامل، ارتباط مستمر و خوبی با کاربران و اعضای شبکه‌ها ایجاد کند و موضوعات و مسائلی را در فضای مجازی مطرح کند که از طرفی در جهت ارتقای امنیت داخلی باشد و از طرف دیگر دشمنان را در موضوع انفعالی و یا دفاعی قرار دهند. اعضای تیم باید قبل از طرح هر نوع مسئله‌ای در شبکه‌های اجتماعی از سوی دیگران به طرح مسئله بپردازند تا دیگران درخصوص مسائل مطرح شده از سوی آنها به بحث و تبادل نظر بپردازند. همچنین آنها باید در صورت طرح شدن مسئله‌ای از سوی دیگران با جدیت به تجزیه و تحلیل آن از منظر خود بپردازند و مسیر گفتگوها را هدایت کنند. البته در این کار باید مواظب باشند دیگران با مطرح کردن موضوعات



انحرافی آنها را مشغول نسازند.

۳. بهره‌گیری از دانشمندان و طراحان جهت طراحی و راه‌اندازی شبکه‌های ملی با برد منطقه‌ای و جهانی: ایران باید بتواند شبکه‌های اجتماعی مجازی جذاب و پرامکاناتی را به کمک دانشمندان توانمند داخلی طراحی و راه‌اندازی کند تا بدین‌وسیله ضمن تشویق دانشمندان به وجود فرصت‌هایی برای فعالیت، کاربران را از عضویت در شبکه‌هایی که منشأ آنها مشکوک است بازدارد. همچنان که می‌دانیم در مورد نیت و قصد طراحان و اداره‌کنندگان شبکه‌های اجتماعی مجازی تردیدهایی است و شواهدی وجود دارد که نشان می‌دهد آنان در مواقعی در خدمت مطامع استعماری قدرت‌های بزرگ قرار گرفته‌اند. بنابراین وجود شبکه‌های اجتماعی مجازی ایرانی - در صورت داشتن امکانات، خوب طراحی شدن و عدم اعمال محدودیت‌های بی‌مورد - می‌تواند بسیاری از اعضای شبکه‌های خارجی را جذب کند.

۴. آموزش خانواده‌ها برای همراهی با فرزندان و نظارت و کنترل و راهنمایی بیشتر: حضور فرزندان در شبکه‌های اجتماعی، درحالی که پدران و مادران آنها اطلاع چندانی از شبکه‌های اجتماعی ندارند و در مواردی حتی از وجود این شبکه‌ها و عضویت فرزندان خود در آنها بی‌خبرند، می‌تواند آسیب‌های جدی و فراوانی بر آنها وارد آورد، ولی در صورت آگاهی پدران و مادران نسبت به شبکه‌ها و نحوه حضور در آنها و به‌ویژه عضویت خود آنها در این شبکه‌ها باعث می‌شود فرزندان در ایجاد ارتباط با اعضای دیگر شبکه و نیز کسب اطلاعات و پذیرش باورها و الگوها محتاط‌تر عمل کرده و با بزرگان خود مشورت کنند. بنابراین برنامه‌هایی از طریق رادیو، تلویزیون، مدرسه و طرق دیگر لازم است تا خانواده‌ها اطلاعات بسیاری نسبت به این شبکه‌ها به‌دست آورند و نظارت بیشتری بر حضور فرزندان خود در شبکه‌ها داشته باشند.

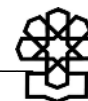
۵. تخصیص بودجه‌های واقعی برای عملی کردن موارد پیش‌گفته: همچنان که در این گزارش دیدیم و در مقاله‌ها و کتاب‌ها و ... نیز می‌بینیم و می‌شنویم و می‌خوانیم شبکه‌های اجتماعی مجازی از ملزومات زندگی امروز هستند و حذف آنها به آسانی مقدور نیست. آنها امکانات زیادی برای زندگی امروزین انسان‌ها در جوامع دارند. همچنین تهدیدات زیادی نیز با خود برای امنیت و هویت جوامع به همراه دارند. برنامه‌ریزی برای مدیریت منابع انسانی جامعه در رابطه با این شبکه‌ها و پیشگیری از تهدیدات ناشی از اینترنت در کل و شبکه‌های اجتماعی بالاخص اجتناب‌ناپذیر و غفلت از این موضوع پشیمان‌کننده است. اما برنامه‌ریزی و اجرای برنامه‌های کاربردی که به تعدادی از آنها نیز اشاره شد جز با تخصیص بودجه‌های کافی ناممکن است. تخصیص بودجه‌هایی که تنها بتوان با آنها اداره‌ای کوچک و چند نفر کارمند آن هم غیرمتخصص را اداره کرد، چندان ثمری ندارد. بلکه

برای تخصیص بودجه برای این کار باید از کارشناسان خبره‌ای که بتوانند برآورد هزینه کنند استفاده شود. همچنین این فکر را که پرداختن به این حوزه جزء اولویت‌های چندم است و فوریتی برای پرداختن به آن نیست باید کنار گذاشت.

۶. **قانونمند کردن استفاده و تأسیس شبکه‌های اجتماعی:** از مهمترین اقدامات در زمینه استفاده مفید و کاهش آسیب‌های شبکه‌های اجتماعی مجازی، تصویب و تهیه قانون مربوط به فعالیت از این فضا و پیش‌بینی مقررات مرتبط می‌باشد که مجلس شورای اسلامی می‌تواند در این راستا نقش بسزایی داشته باشد.

پی‌نوشت‌ها

۱. کاستلن، مانوئل. عصر اطلاعات: اقتصاد، جامعه و فرهنگ (جلد دوم، قدرت هویت)، ترجمه حسن چاوشیان، تهران، طرح نو، ۱۳۸۵.
۲. شاقاسمی، احسان. مروری بر زمینه‌های تأثیر فضای مجازی بر نظریه‌های ارتباطات، مجله جهانی رسانه، ش ۲، پاییز ۱۳۸۵، در <http://gmj.ut.ac.ir/maghale.aspx?id=36>
۳. مولایی، محمدمهدی. شبکه‌های اجتماعی مجازی، هفته‌نامه پنجره، ش ۵۹.
۴. ویکی‌پدیا (فارسی)، زیرعنوان: شبکه‌های اجتماعی.
۵. همان.
۶. افتخاری، اصغر. معنا و مقام امنیت نرم در گفتمان اسلامی، درآمدی بر نظریه دفاعی الهی، در امنیت نرم در جمهوری اسلامی ایران (مجموعه مقالات)، معاونت پژوهشی دانشکده امام هادی (ع)، ۱۳۸۸، ص ۲۵.
۷. تهامی، سیدمجتبی. امنیت ملی؛ داکترین، سیاست‌های دفاعی و امنیتی، تهران، نشر آجا، ۱۳۸۴، ص ۷۸.
۸. باقری سیامک و جعفر، یوسفی. چپستی تهدید نرم، در: امنیت نرم در جمهوری اسلامی ایران (مجموعه مقالات)، معاونت پژوهشی دانشکده امام هادی (ع)، ۱۳۸۸، ص ۵۰.
۹. همان.
۱۰. عباسی، محمد. جستاری نظری به مفاهیم قدرت و امنیت نرم، در: امنیت نرم در جمهوری اسلامی ایران (مجموعه مقالات)، معاونت پژوهشی دانشکده امام هادی (ع)، ۱۳۸۸، ص ۲۳۰.
۱۱. لطفی، صفرعلی. ماهیت تهدید نرم در گفتمان امنیتی اسلام، در: امنیت نرم در جمهوری اسلامی ایران (مجموعه مقالات)، معاونت پژوهشی دانشکده امام هادی (ع)، ۱۳۸۸، ص ۱۴۱.
۱۲. ایمانی، جاوید. نشانه‌شناسی تهدید نرم ویژه جنگ رسانه‌ای، در: همان، صص ۲۹۲-۲۷۹.
۱۳. چالش‌های فرهنگ و هویت در فضای مجازی، در: www.rasekhoon.net/article/show-49193.aspx
۱۴. مروری بر تاریخچه فیس‌بوک ... همان.
۱۵. دریفوس، هیوبرت. نگاهی فلسفی به اینترنت، ترجمه علی ملائکه، تهران، گام نو، ۱۳۸۳، ص ۱۳۰.
۱۶. استفاده دختران جوان از اینترنت و تأثیر آن بر هویت دینی، در: www.tebgan.net/index.aspx?pid=9348article ID=458785



۱۷. کاستلن، ص ۳۱۲.
۱۸. جمعی از نویسندگان، مجموعه مقالات همایش رسانه‌ها و ثبات سیاسی - اجتماعی جمهوری اسلامی ایران، تهران، پژوهشکده مطالعات راهبردی، چاپ اول، ۱۳۸۱، ص ۲۲۰.
19. International Strategy for Cyberspace; Prosperity, Security, and Openness in a Networked world, May 2011.
۲۰. جمعی از نویسندگان، ص ۲۳۵.
۲۱. مدیرعامل توییتر عضو گروه مشاوران اوباما شد، در:
<http://socialmedia.ir/?p=194>
۲۲. فیس‌بوک چگونه برای آمریکا جاسوسی می‌کند، در:
<http://alef.ir/138/content/view/103515>
۲۳. همان.
۲۴. دیپلماسی دیجیتال به ابزار نوین آمریکا در دیپلماسی عمومی تبدیل شده است، در:
www.gerdab.ir/fa/news/1569
۲۵. کمک ۵۰ میلیون دلاری علیه فیلترینگ شبکه‌های اجتماعی، در:
www.tebgon.net/index.aspx?pid=163133
۲۶. شبکه‌های اجتماعی، اهرم آمریکا برای افزایش اختلافات خارجی، در:
www.psgop.ir/?p=4896
۲۷. پیشبرد اهداف ارتش آمریکا با دیپلماسی دیجیتال در خاورمیانه، در:
www.gerdab.ir/fa/news/2324
۲۸. رژیم صهیونیستی و استفاده از فضای مجازی، در:
www.psyop.ir/?p=1557
۲۹. استراتژی رسانه‌ای ارتش آمریکا در شبکه‌های اجتماعی در سال ۲۰۱۰، در:
www.sistema.com/Nsite/Fullstory/News/?Id=805
۳۰. ضیایی‌پرور، حمید و سیدوحید عقیلی. بررسی نفوذ شبکه‌های اجتماعی مجازی در میان کاربران ایرانی، فصلنامه رسانه، سال بیستم، ش ۴، شماره پیاپی ۸۰، زمستان ۱۳۸۸.
۳۱. همان.
۳۲. جمعی از نویسندگان، صص ۲۲۷-۲۲۹.
۳۳. همان.
۳۴. تلاش سایبری کاخ سفید در جنگ نرم، در:
www.resalay-news.com/fa/?code=27390
۳۵. همان.
۳۶. متن کامل گزارش مؤسسه تحقیقات خاور نزدیک واشنگتن درباره جنگ نرم با ایران، در:
www.ghatreh.com/News/4879109.html
۳۷. همان.
۳۸. چگونه شبکه‌های اجتماعی به آشوب‌ها در ایران شکل دادند؟، در:
<http://rajanews.com/detail.asp?Id=39502>
۳۹. توییتر فارسی برای مخالفت با ایران راه‌اندازی شده است، در:
www.webgardi2030.ir/news/90
۴۰. نقش فیس‌بوک در اغتشاشات اخیر، در:
www.fardanews.com/fa/news/105406

۴۱. همان.

۴۲. جمعی از نویسندگان، ص ۵۹.

۴۳. ضیایی پرور، حمید. جنگ نرم، ویژه جنگ رسانه‌ای، تهران، مؤسسه فرهنگی مطالعات و تحقیقات

بین‌المللی ابرار معاصر تهران، ۱۳۸۳، صص ۱۴۷-۱۵۷.

۴۴. سعادت، علی. همان، ص ۲۲۳.

۴۵. همان، صص ۲۲۱-۲۲۲.



مرکز پژوهش‌ها
مجلس شورای اسلامی

شماره مسلسل: ۱۲۲۳۶

شناسنامه گزارش

عنوان گزارش: تأثیر شبکه‌های اجتماعی مجازی بر امنیت ملی

نام دفتر: مطالعات سیاسی (گروه سیاست داخلی)

تهیه و تدوین: خیراله خیری اصل

ناظر علمی: ابوزر گوهری مقدم

متقاضی: معاونت پژوهشی

ویراستار: حسین صدری نیا

ویراستار ادبی: فرزاد جعفری

واژه‌های کلیدی: —

تاریخ انتشار: ۱۳۹۰/۱۱/۲۴