بایسته‌های توسعه امنیت نرم در فضای مجازی با تأکید بر شبکه‌های اجتماعی

افشین راسخی[1]

از صفحه ۱ تا صفحه ۳۹

فصلنامه مطالعات حفاظت و امنیت انتظامی

تاریخ دریافت: ۹٤/۰۹/۲۰

تاریخ پذیرش: ۹۵/۰۲/۱۰

چکیده

گستره مفهوم امنیت در شبکه، در پنج حوزه سیاسی، اقتصادی، فرهنگی، اجتماعی و قضایی ریشه دوانده که فقدان بسته سیاستی منسجم برای مدیریت پیشگیرانه تهدیدهای احتمالی در فضای مجازی، می‌تواند زیربنای توسعه مطلوب را با چالش‌های جدّی مواجه کند، رفع خلأهای تقنینی، نظارتی و اجرایی مدیریت تهدیدهای امنیت اجتماعی در فضای وب، زمانی دارای ضریب اثربخشی بالایی است که از شش مشخصهٔ: هم‌سویی با اسناد بالادستی، فرابخشی، کلان‌نگری، راهبردی، هدف‌محوری (انسجام فکری) و برنامه‌محوری (ثبات رویه‌ای) برخوردار باشد و هر گونه نگاه سطحی نسبت به تهدیدهای محیط مجازی، می‌تواند نطفه شکل‌گیری وقوع بحران‌های پنج‌گانه منزلت، مشروعیت، نفوذ، توزیع و مشارکت را در سیاست‌های کلان به‌وجود آورد.

امروزه شبکه‌های اجتماعی مجازی که محصول پیشرفت فناوری در حوزه اینترنت می‌باشند، از جایگاه ویژه‌ای در جنگ نرم برخوردارند. اهمیت این‌گونه شبکه‌ها تا آنجاست که به‌عنوان یکی از ابزارهای براندازی و فروپاشی از درون، در دستورکار بسیاری از کشورهای متخاصم قرار گرفته است؛ هرچند که خود از تهدیدها و آسیب‌های این‌گونه شبکه‌ها در امان نیستند. شبکه‌های اجتماعی مجازی، به‌دلیل خصلت افقی بودنشان، از عدم رهبری رنج می‌برند و نیروی هدایت‌کننده در آن‌ها وجود ندارد، بنابراین هریک از اعضای شبکه ممکن است براساس نظر و دیدگاه شخصی‌اش عمل کند یا اینکه به رفتار دیگران رجوع کند و از آن الگوبرداری نماید.

در این نوشتار بر آن شدیم با بیان اهمیت رسانه‌های نوین و آشنایی خوانندگان محترم با جنگ سایبری و مشخصات آن، شبکه‌های اجتماعی مجازی را به‌عنوان یکی از ابزارهای جنگ سایبری به تفصیل تبیین نماییم. اینکه شبکه‌های اجتماعی مجازی اساساً چه نوع شبکه‌هایی است و چه دسته‌بندی‌هایی دارد، موضوع اولیه این نوشتار است. در ادامه تهدیدهای امنیتی این شبکه‌ها و راه‌های مقابله با آن را بازگو خواهیم کرد.

کلیدواژه‌ها: *امنیت ملی، تهدیدهای نوین، جنگ سایبری، جنگ نرم، رسانه‌های نوین، شبکه‌های اجتماعی.*

---

۱. کارشناس قضایی و فارغ‌التحصیل دانشکده افسری ـ faslname.motaleat@ chmail.ir

مقدمه

واقعیت امر این است که امروزه زیرساخت‌های حیاتی کشورها در زمینه‌های مختلف، وابستگی شدیدی به ارتباط در فضای مجازی پیدا نموده‌اند؛ هرچند تهدیدها و چالش‌های جدید، پیچیده، مبهم و خطرناک در تمامی حوزه‌ها نیز ایجاد نموده و درواقع امنیت ملی کشورها را به مخاطره انداخته است. بنابراین اینترنت و بروز شبکه‌های اجتماعی را باید مهم‌ترین پدیده‌ای دانست که بخش اعظم حیات انسان را در عصر حاضر تحت‌تأثیر قرار داده و در آینده نیز تأثیرات آن به مراتب بیشتر خواهد شد و این پدیده موضوع بیشتر فعالیت‌های علمی و عملی انسان‌ها در آینده است.

این پدیده از بار امنیتی بالایی برخوردار است، تا آنجا که امریکا و برخی کشورهای پیشرفته، تدوین راهبرد امنیت فضای سایبر[1] را در دستورکار خود قرار داده، به‌صورت جدی پیگیر این امر و مباحثی چون جنگ اطلاعاتی[2] بوده و از جنگ اطلاعات با عنوان جنگ نامتقارن، چهره جدید جنگ‌ها تعبیر می‌نمایند، زیرا اینترنت و شبکه‌های اجتماعی باعث تحول و دگرگونی عظیمی در نوع تهدیدها، شیوه‌های عملیات اطلاعاتی، جاسوسی، ساختار دستگاه‌های اطلاعاتی، نظامی و... شده است. آثاری نظیر جنگ اطلاعاتی، سرقت اطلاعات، تخریب اطلاعات، جاسوسی آسان و سریع، تقویت تروریسم، ضعف امنیتی، تأثیرات مخرب اقتصادی، اجتماعی، فرهنگی و... حاصل بهره‌گیری غیرصحیح از شبکه‌های موجود در فضای مجازی است.

از سوی دیگر، ارتباطات، سنگ‌پایه اولیه تمدن و یکی از ویژگی‌های سازمان بشری است. ارتباطات جمعی به‌عنوان یک نهاد اجتماعی، با دیگر نهادهای موجود در جامعه روابط متقابلی

1. Cyber
2. Intelligence warfare

دارد. بدون شک، این نهاد مهم اجتماعی عامل مهمی در تغییر و تحولات اجتماعی، سیاسی و امنیتی تلقی می‌شود. نظام ارتباطی پدیده‌ای است جهانی که در همه‌جا وجود دارد و به نیازهایی پاسخ می‌دهد که برای تمامی افراد مشترک است. درواقع یک جامعه انسانی متعالی نمی‌تواند بدون نظام ارتباطی به حیات خود ادامه دهد. با توسعه جوامع انسانی و حرکت از سادگی به‌سمت پیچیدگی، مسئله ارتباطات و تبادل، پیچیده‌تر شده و اهمیت بیشتری می‌یابد.

«التوسر» رسانه‌های ارتباط جمعی را به‌عنوان بخشی از دستگاه‌های ایدئولوژیک از ابزارهای اساسی قدرت حاکم می‌داند که می‌توانند با ارائه تصویرهای مطلوب نظام جهانی یا اجتماعی، اندیشه مناسب را بازتولید نمایند (روحانی، ۱۳۸۷: ۲۹) و در همین راستا شبکه‌های اجتماعی مجازی که با سرعتی بی‌بدیل درحال گسترش بوده و مورد اقبال نسل جدید واقع شده است، به‌عنوان ابزار جنگ نرم برای انقلاب‌های رنگین در کشورهای غیر همسو استفاده می‌شود. کشورمان ایران نیز به‌عنوان یکی از کشورهای غیر همسو با منافع ایالات متحده متأثر از تهدیدهای جنگ نرم در فضای سایبری بوده است.

شبکه‌های اجتماعی چون فیسبوک، اورکات، یوتیوپ، توئیتر و... بستری جدید برای ایجاد ارتباطات مجازی بین افراد هستند که در مدت زمان کوتاهی در ایران به سرعت رشد کرده‌اند (کوک و هاپکینز، ۱۳۸۸: ۲۰)، درنتیجه مشکلات و ابهامات بسیاری در این حوزه ظهور یافته و اذهان محققان و نخبگان زیادی را در جهان معطوف و مشغول به خود نموده است. از جمله اینکه نمی‌توانیم رابطه شبکه‌های اجتماعی موجود در فضای سایبری را با اطلاعات برقرار کنیم، نمی‌دانیم چه بخشی از اطلاعات مختل می‌شود یا آسیب می‌بیند، نمی‌دانیم چگونه می‌توانیم بین حفاظت‌اطلاعات و امکانات ارتباط برقرار کنیم، نمی‌دانیم آسیب‌ها و تهدیدهای این پدیده برای حفاظت از اطلاعات چیست؟ و...

پاسخ به هریک از این ابهامات و مشکلات نیازمند یک بررسی مفصل می‌باشد که در این مقاله تنها به یک موضوع، یعنی بایسته‌های توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی مجازی پرداخته شده است.

الف. کلیات

۱/الف. بیان مسئله

هزاره سوم را عصر دانایی نامیده‌اند. اقتصاد جدید عبارت است از «داد و ستد دانش». دانایی، سرمایه را فراهم آورده و پایه‌های قدرت فردی و سازمانی را تشکیل می‌دهد. اطلاعات موجود هر سه یا چهار سال، دو برابر می‌شود. قدرت تفکر، به‌عنوان باارزش‌ترین دارایی سازمانی تلقی می‌شود. این دانش تعیین‌کننده وضعیت رقابتی در جهان است. درحال حاضر بزرگ‌ترین چالش مدیران علاوه بر ایجاد سرمایه دانایی، امن‌سازی آن است (یوسفی، ۱۳۸۴: ۲).

شبکه جهانی اینترنت با ارائه سرویس‌های بی‌بدیل و متنوع، بستر مناسبی را برای مبادله اطلاعات و توسعه دانش و دانایی فراهم کرده و بسیاری از محققان و دانشمندان با بهره‌گیری از امکانات متنوع این بستر ارتباطی، دامنه پژوهش و تحقیقات خود را در سراسر جهان گسترش داده و به مبادله اطلاعات و دانش می‌پردازند.

از سوی دیگر باید باور داشته باشیم که واقعیت این است که با رشد سریع فناوری‌های ارتباطی و تحولات عمده در حوزه به‌کارگیری ابزارهای نوین با هدف براندازی نظام‌های سیاسی غیر همسو، جنگ نرم علیه کشورمان در فضای سایبر طی سال‌های اخیر و با کمک شبکه‌های اجتماعی مجازی ابعاد وسیع و عمیقی به خود گرفته است.

مسئله‌ای که در این نوشتار طرح شده، تبیین کارکردهای شبکه‌های اجتماعی مجازی و احیاناً تهدیدهای نرم آن‌ها در فضای سایبری می‌باشد، چرا که به‌نظر می‌رسد این فناوری نوین تأثیر بسیار شگرفی در پیوندهای اجتماعی در فضای مجازی به‌خصوص در مواقع بحرانی دارد و می‌تواند در این مواقع کارکردهای متفاوتی داشته باشد.

درنتیجه می‌توان گفت همان‌گونه که شبکه‌های مجازی تعبیه شده در فضای سایبری، یک فرصت ایده‌آل برای توسعه اطلاعات محسوب می‌شود، ابزاری مناسب برای حمله به اطلاعات قلمداد می‌گردد. بنابراین قبل از استفاده از این دسته از شبکه‌ها برای تبادل اطلاعات و... باید این پدیده را به‌درستی شناخت و به این پرسش، پاسخ داد که بایسته‌های توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی کدام‌اند؟.

۲/الف. ضرورت و اهمیت تحقیق

در بسیاری از موارد کاربران اینترنت و شبکه‌های اجتماعی مجازی در رایانه شخصی یا گوشی همراه خود، اطلاعات باارزشی مانند فیلم، تصاویر خانوادگی و... را نگهداری می‌کنند که به‌هیچ‌وجه مایل به افشا یا دسترسی غیرمجاز به آن‌ها نیستند. در این حالت، اطلاعات شما در معرض تهدیدهای بی‌شمار اینترنت از جمله دسترسی غیرمجاز، افشا، تغییر، نابودی و... قرار می‌گیرد. بنابراین ضرورت دارد که قبل از استفاده از اینترنت و شبکه‌های اجتماعی موجود در آن، تهدیدهای آن را شناخت و در جهت مهار آن‌ها اقدام کرد.

ازآنجاکه نتایج این تحقیق می‌تواند برای ارائه بایسته‌های توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی مجازی مفید واقع شود، دارای اهمیت بوده و به دلایل زیر، انجام آن امری ضروری است:

- شناخت فضای مجازی و ویژگی‌های آن؛
- چیستی، چگونگی و کارکردهای شبکه‌های اجتماعی مجازی؛

- شناسایی تهدیدهای متصور بر امنیت اطلاعات به هنگام استفاده از اینترنت و شبکه‌های اجتماعی؛
- تهدیدها و چالش‌های شبکه‌های اجتماعی مجازی در حوزه‌های گوناگون؛
- معرفی شبکه‌های اجتماعی فعال و دلایل استقبال کاربران ایرانی از شبکه‌های اجتماعی؛
- کارکرد شبکه‌های اجتماعی در مراحل مختلف جنگ نرم؛
- معرفی و ارائه الگوی امنیت اطلاعات در فضای مجازی.

۳/الف. هدف‌های تحقیق

هدف اصلی: شناسایی بایسته‌های توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی.

هدف‌های فرعی:

- شناخت فضای مجازی و تهدیدهای متصور بر امنیت اطلاعات به هنگام استفاده از اینترنت و شبکه‌های اجتماعی؛
- بازشناسی کارکردهای شبکه‌های اجتماعی مجازی و تهدیدها و چالش‌های شبکه‌های اجتماعی مجازی در حوزه‌های گوناگون؛
- معرفی شبکه‌های اجتماعی فعال و دلایل استقبال کاربران ایرانی از شبکه‌های اجتماعی؛
- شناخت کارکرد شبکه‌های اجتماعی در مراحل مختلف جنگ نرم؛
- معرفی الگوی امنیت اطلاعات در فضای مجازی.

٤/الف. سؤال‌های تحقیق

سؤال اصلی: بایسته‌های توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی کدام‌اند؟

سؤال‌های فرعی:

- فضای مجازی و تهدیدهای متصور بر امنیت اطلاعات به هنگام استفاده از اینترنت و شبکه‌های اجتماعی کدام‌اند؟
- کارکردهای شبکه‌های اجتماعی مجازی و تهدیدها و چالش‌های شبکه‌های اجتماعی مجازی در حوزه‌های گوناگون کدام‌اند؟
- شبکه‌های اجتماعی فعال و دلایل استقبال کاربران ایرانی از شبکه‌های اجتماعی کدام‌اند؟
- کارکرد شبکه‌های اجتماعی در مراحل مختلف جنگ نرم چیست؟
- الگوی امنیت اطلاعات در فضای مجازی چیست؟

۵/الف. روش تحقیق

تحقیق حاضر از نوع تحلیلی ـ استنباطی است.

ب. ادبیات نظری

۱/ب. تعاریف و اصطلاح‌ها

فضای مجازی و ویژگی‌های آن

فضای مجازی به شبکه واقعیت مجازی به اشتراک گذاشته شده و بسیار پیشرفته گفته می‌شود. این مفهوم برگرفته از تخیلات ویلیام گیبسون در رمانی با عنوان (Neuromancer, ۱۹۸۲) است. به‌عبارت دیگر، فضای مجازی به تمامی محیط‌هایی مانند اینترنت که در آن اشخاص توسط رایانه‌های به‌هم پیوسته با یکدیگر در ارتباط هستند، گفته می‌شود. یکی از ویژگی‌های فضای مجازی، برقراری ارتباط مستقل از فاصله فیزیکی است (حسنوی، ۱۳۸۱: ۱۵۱).

فضای مجازی[1] از جمله مفاهیم مورد استفاده در حوزه فناوری اطلاعات و ارتباطات است. نوربرت وینر (بنیان‌گذار علم سایبرنتیک) در کتاب «سایبرنتیک و جامعه» می‌گوید

1.Cyber Space

که سایبرنتیک از واژه یونانی کوبرنتس[1] به‌معنای سکاندار که منشأ آن واژه انگلیسی گاورنر[2] است، اقتباس شده است. وی معتقد است که پیش از آن نیز این واژه در سده ۱۹ توسط آمپر در اشاره به مفهومی در علوم سیاسی مورد استفاده قرار گرفته است. در تعریف سایبرنتیک، وینر ارتباط‌گیری و کنترل را به‌طور توأمان دخیل دانسته است، چرا که معتقد است زمانی‌که فرد با شخص دیگری درحال برقراری ارتباط بوده و پیامی را برای او می‌فرستد و طرف مقابل پیام وابسته‌ای را به فرد باز می‌گرداند که حاوی اطلاعاتی بوده که در آغاز در دسترس او قرار داشته، این فرایند لازمه‌اش وجود میزان خاصی از کنترل طرفین بر ارتباط و آگاهی از پیام است.

درک مفهوم فضای مجازی بدون درک مفهوم فضا و اهمیت آن در جهان امروز بی‌معناست. در حقیقت فضای مجازی مانند هر فضایی دارای موقعیت جغرافیایی، فیزیکی یا محدوده سرزمینی خاص نیست، ولی با این وجود نوعی واقعیت برجسته در جهان معاصر است، چرا که ما کنشگران انسانی هر روزه در آن دست به عمل می‌زنیم، با آن در تعامل هستیم، از آن یاری می‌طلبیم و با او به داد و ستد اطلاعات می‌پردازیم.

ظهور جهان جدید یعنی جهان مجازی، بسیاری از روندها و نگرش‌ها و ظرفیت‌های آینده جهان را تحت‌تأثیر خود قرار می‌دهد. این جهان درواقع به موازات و گاه حتی بر جهان واقعی مسلط شده و عینیّت واقعی پیدا می‌کند. این دو جهان دارای داد و ستدهای بی‌شماری با یکدیگر هستند. جهان واقعی با خصایصی مانند داشتن جغرافیا، دارای نظام سیاسی خاص بودن، محبوس بودن، طبیعی‌بودن و... از جهان مجازی متمایز می‌شود و جهان مجازی نیز در مقابل با خصیصه‌هایی مثل بی‌مکانی، فرا زمان بودن، تکثر داشتن،

1. KUBERNETS
2. GOVERNER

به‌طور همزمان قابل دسترس بودن و... از جهان واقعی به‌طور نسبی جدا می‌شود. ازنظر «عاملی» مهم‌ترین تغییری که فضای دو جهانی یا به‌عبارتی دیگر، ظهور فضای مجازی و در پرتوی آن شکل‌گیری جهان مجازی به‌وجود آورده، تغییر در روابط انسانی است؛ جایگزینی روابط چهره به چهره سنتی با روابط مجازی با واسطه رایانه، شاید مهم‌ترین بخش این تغییر است که در جای خود بیشتر بدان خواهیم پرداخت.

امنیت فضای مجازی

امنیت ازنظر لغوی از ریشه امن و به‌معنای آرامش و اطمینان خاطر و در مقابل خوف و هراس داشتن است. مفهوم امنیت در فضای مجازی باتوجه به هدف‌های امنیت، در این فضا قابل تعریف است (جمال‌پور، ۱۳۸۴: ۲۴).

شبکه‌های اجتماعی

مفهوم شبکه اجتماعی نخستین بار در سال ۱۹۴۰ در انسان‌شناسی توسط براون معرفی شد. سپس در اواسط دهه ۱۹۵۰ این مفهوم توسط بات و بارنز مورد استفاده قرار گرفت (چلبی، ۱۳۷۳:۱۰).

یک شبکه اجتماعی، یک ساختار متمرکز اجتماعی است که از گره‌هایی، اغلب به‌عنوان فرد یا سازمان تشکیل شده است. این گره‌ها توسط یک یا چند نوع خاص از وابستگی به‌هم متصل می‌شوند. مثال‌هایی از وابستگی‌ها می‌تواند اشتراک‌ها، علایق، ایده‌ها، تبادلات مالی، دوستی، خویشاوندی، تجاری، لینک‌های وب، مسافرت و یا سرایت بیماری‌ها باشد. ساختارهای حاصل از شبکه‌های اجتماعی اغلب بسیار پیچیده هستند. در تحلیل شبکه‌های اجتماعی، گره‌ها همان افراد درون شبکه‌ها هستند و رشته‌ها روابط میان آن‌هاست. انواع زیادی از رشته‌ها می‌تواند میان گره‌ها وجود داشته باشد (tapscptt, ۲۰۰۹: ۳۶).

۲/ب. اهم تهدیدهای فضای سایبری

جنگ نرم[1]

اگر جنگ نرم را شامل جنگ اطلاعات، جنگ رایانه‌ای، جنگ الکترونیک، جنگ رسانه‌ای، جنگ روانی و جنگ شبکه‌ای بدانیم؛ باید گفت که اینترنت بستر مناسبی برای این میدان جدید نبرد است.

فعالیت‌های اطلاعاتی (جاسوسی)

جاسوسی رایانه‌ای ناظر بر کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی و نظامی و نیز افشا، انتقال و استفاده از اسرار است که به‌شکل ورود به سیستم، پردازش داده‌ها و اعمال مشابه رخ می‌دهد. از ویژگی‌های جاسوسی رایانه‌ای می‌توان به موارد زیر اشاره کرد:

- محدوده اسرار در جاسوسی رایانه‌ای شامل اسرار نظامی، سیاسی، تجاری، اقتصادی و... است؛
- تمامی مراحل جاسوسی که به‌شکل تفتیش غیرمجاز، افشا، انتقال، استفاده از ترفندهای برنامه‌نویسی و استفاده از ترفندهای نفوذ است، در رایانه رخ می‌دهد؛
- در جاسوسی رایانه‌ای وجود ارکان تشکیل شده فضای مجازی امری لازم است؛
- در جاسوسی رایانه‌ای ممکن است جاسوسی فقط به‌دلیل ضعف سیستم‌های امنیتی انجام شود و فرد دومی وجود نداشته باشد.

جمع‌آوری اطلاعات، دست‌اندازی به حریم خصوصی افراد، استخدام جاسوس، ملاقات‌های اطلاعاتی، فعالیت‌های اطلاعاتی و جاسوسی در اینترنت اغلب ازطریق سازمان‌های اطلاعاتی و صاحبان اینترنت و در قالب سرویس‌دهندگان، موتورهای جست‌وجو، وب‌سایت‌های امنیتی و وب‌سایت‌های خدماتی صورت می‌گیرد. یکی از

1. Information Warforce (IW)

مشهورترین موتورهای جست‌وجو، «گوگل» است. موتور جست‌وجوی گوگل که در سال ۱۹۹۸ تأسیس شد، اندک‌اندک جای خود را بین سایر رقبا باز کرد.

استفاده از الگوریتم‌های جدید که دقت جست‌وجو را تا حد زیادی بالا می‌برد، باعث شد تا گوگل کفه بازار موتورهای جست‌وجو را به نفع خود سنگین کند. توانایی خارق‌العاده گوگل در جست‌وجوی وب، ایجاد فهرستی از محتوای سایت‌های مختلف، زمان کوتاه جست‌وجو و سرعت بالای ارسال نتایج، از نکته‌های قوّت گوگل است.

درحال حاضر بیش از ۷۵ درصد ورود به بسیاری از سایت‌ها ازطریق گوگل است. سیستم آگهی منحصربه‌فرد گوگل در موفقیت روزافزون و کسب درآمدهای چند صد میلیون دلاری در سال، نقش بسزایی داشته است. برخلاف روش‌های سنتی تبلیغ ــ که بدون توجه به نیازهای کاربر، به یک‌باره صفحات تبلیغاتی در برابر کاربر ظاهر می‌شوند و گاهی این روش‌ها می‌توانند ضد تبلیغ هم باشند ـ در این روش، تبلیغات کاملاً متناسب با نیازهای مخاطب صورت می‌گیرد. به‌عنوان مثال وقتی کاربر در سایت گوگل اقدام به جست‌وجو در مورد «رباتیک» می‌کند، تبلیغ میزبانی وب در برابرش ظاهر نمی‌شود. در قسمت سمت راست صفحه کادری برای تبلیغ درنظر گرفته شده که سایت‌هایی متناسب با کلمات کلیدی جست‌وجو به‌صورت متنی و مجزا از نتایج جست‌وجو به کاربر معرفی می‌شوند. همزمان با بزرگ‌ترشدن گوگل و گسترش حوزه‌های فعالیت آن، نقد صاحب‌نظران و مدافعان حوزه خصوصی افزایش یافت. در رأس منتقدان گوگل سازمان‌هایی مانند PI قرار دارد که اتهام‌های سنگینی را متوجه گوگل کرده است (گروه امداد امنیت رایانه ایران)[1].

1. http://www.ircert.com

اتهام‌هایی که PI به گوگل وارد کرده مبتنی بر ۹ ماده است:

- کوکی‌های گوگل مادام‌العمر هستند؛
- گوگل همه چیز را ذخیره می‌کند؛
- گوگل به‌صورت نامحدود داده‌های کاربران را ذخیره می‌کند؛
- گوگل تاکنون مشخص نکرده است که به چه دلیل به این داده‌ها نیاز دارد؛
- گوگل نیروهای امنیتی را به استخدام خود درآورده است؛
- نوار ابزار گوگل جاسوسی می‌کند؛
- ذخیره‌سازی نسخه Cahce غیر قانونی است؛
- گوگل با کاربران خود، برخورد دوستانه‌ای ندارد؛
- گوگل بمب ساعتی از بین برنده حریم خصوصی است.

فعالیت‌های سیاسی

بسیاری از گروهک‌ها و حزب‌های سیاسی مجاز و غیرمجاز، از امکانات اینترنت به‌منظور فعالیت‌های سیاسی مانند جذب نیرو، هدایت، آموزش، تجمع و راهپیمایی استفاده می‌کنند. در بسیاری از موارد گروه‌های سیاسی با بهره‌گیری از روش‌های تبلیغاتی، کاربران را به انحراف می‌کشانند.

فساد و فحشا

برخی از مظاهر فساد و فحشا که در اینترنت رونق زیادی دارد عبارت‌اند از:

- وب‌سایت‌ها و وبلاگ‌های مستهجن؛
- نشر مطالب مستهجن و توهین‌آمیز علیه افراد؛

- پورنوگرافی؛
- کلاهبرداری؛
- جعل؛
- دسترسی غیرمجاز؛
- تخریب رایانه‌ای؛
- خرابکاری رایانه‌ای (سابوتاژ)؛
- افشای حریم خصوصی و جریان آزاد اطلاعات؛
- جرائم سازمان‌یافته؛
- جرائم رایانه‌ای؛
- نفوذگران؛

برنامه‌های مزاحم

در شبکه جهانی اینترنت به‌طور گسترده از برنامه‌های مزاحم مانند کرم‌ها، اسب‌های تروا و ویروس‌ها استفاده می‌شود، اما برخی از برنامه‌های مزاحم در اینترنت استفاده گسترده‌تری دارند که از آن جمله می‌توان به بدافزارهای زیر اشاره کرد:

شماره‌گیرها

این‌گونه برنامه‌ها وظیفه‌شان ارتباط دادن کاربر ازطریق خط تلفن به سرورهایی در دیگر کشورها برای دسترسی مستقیم به اطلاعات آن‌هاست. این سرورها معمولاً مربوط به سایت‌های غیراخلاقی بوده و برقراری ارتباط با آن‌ها ازطریق خط تلفن باعث هزینه بسیار زیاد مالی می‌شود.

جاسوس‌افزارها

جاسوس‌افزارها نرم‌افزارهایی هستند که بر روی رایانه شما نصب و اجرا شده و فعالیت‌های شما را به طرق مختلف مانند: عکس‌برداری، فیلم‌برداری، ممیزی ثبت می‌کنند یا اطلاعات

موجود بر روی آن را به‌طور پنهانی جمع‌آوری کرده و در اختیار نفوذگران قرار می‌دهند. نوع اطلاعاتی که از رایانه شما جمع‌آوری می‌شود، متفاوت است. بعضی نرم‌افزارهای جاسوسی فقط اطلاعات سیستمی شما را ردیابی می‌کنند، مانند نوع اتصال به اینترنت یا نوع سیستم عامل، برخی نیز اطلاعات فردی را جمع‌آوری می‌کنند، مانند ردگیری عادت‌ها و علایق شما هنگام کار با اینترنت و بالاخره گاهی بدتر با فایل‌های شخصی شما سروکار دارند. نرم‌افزار جاسوسی بدون رضایت و اطلاع کاربر نصب می‌شود.

مراحل نصب نرم‌افزار جاسوسی روی رایانه شما می‌تواند با مشاهده یک وب‌سایت، دیدن یک نامه الکترونیکی به فرمت اچ‌تی‌ام‌ال[1] یا با کلیک‌کردن یک پنجره بازشونده[2] آغاز شود.

انواع زیادی از این نوع نرم‌افزارها در اینترنت فعال هستند، اما می‌توان آن‌ها را به دو گروه عمده تقسیم کرد:

جاسوس‌افزارهای خانگی[3]

نرم‌افزاری است که اغلب توسط صاحبان رایانه‌ها به‌منظور آگاهی از تأثیر اینترنت بر روی شبکه‌های رایانه‌ای خودی، نصب می‌شود. مدیران از این نرم‌افزار برای آگاهی از فعالیت‌های برخط کارمندان استفاده می‌کنند. بعضی از افراد نیز برای اطلاع از فعالیت‌های سایر اعضای خانواده استفاده می‌کنند، مانند مشاهده محتوای اتاق‌های گفت‌وگوی فرزندان. یک شخص ثالث نیز می‌تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب رایانه، نصب کند. مجریان قانون از نرم‌افزارهای جاسوسی برای آگاهی از فعالیت مجرمانی استفاده می‌کنند که همین مجرمان خود از این نرم‌افزارهای جاسوسی برای به‌دست آوردن اطلاعات از رایانه‌های شخصی دیگران به قصد دزدی دارایی‌های آن‌ها استفاده کرده‌اند.

1. HTML
2. pop-up
3. Domestic Spyware

جاسوس‌افزارهای تجاری[1]

نرم‌افزارهایی که برای تعقیب فعالیت‌های کاربران اینترنت استفاده می‌شود. برخی از جاسوس‌افزارها عبارت‌اند از:

✓ ثبت‌کنندگان نشانی‌های وب و صفحات نمایش

ثبت‌کنندگان نشانی‌های وب، وب‌سایت‌ها و صفحات دیده‌شده را ردیابی می‌کنند. ثبت‌کنندگان صفحه نمایش می‌توانند یک تصویر سیاه و سفید کوچک (برای کم‌کردن حجم تصویر) از صفحه پیش روی شما در هر زمان بگیرند و این تصاویر را بدون اطلاع شما ذخیره کنند یا بفرستند. این روش‌ها برای جاسوسی‌های خانگی متداول است.

✓ ثبت‌کنندگان چت و نامه الکترونیکی

این ثبت‌کنندگان یک تصویر متنی از تمام نامه‌های الکترونیکی واردشونده، خارج‌شونده و چت‌ها تهیه می‌کنند.

✓ ثبت‌کنندگان کلید[2] و کلمات عبور

هنگامی که شما مشغول کار با رایانه هستید، یک نفر بالای سر شما ایستاده و بر اعمال شما نظارت می‌کند! ثبت‌کننده کلمه عبور این کار را می‌کند، یعنی کلمات عبور تایپ‌شده را ردگیری می‌کند، اما ثبت‌کننده کلید تمام آنچه را که تایپ می‌شود، ثبت نمی‌کند.

✓ حشرات وبی

حشرات وبی به‌عنوان جاسوسان تبلیغ‌کننده یا نرم‌افزارهای تبلیغ شناخته می‌شوند. هنگامی که شما چنین نرم‌افزاری روی رایانه خود دارید، بعد از انجام بعضی از کارها، مانند تایپ‌کردن عبارت‌هایی در یک موتور جست‌وجو، پنجره‌های بازشونده تبلیغاتی خاصی

1. Commercial Spyware
2. Keyloger

را مرتبط با عناوین مورد جست‌وجو دریافت می‌کنید. گاه این تبلیغات حتی زمانی‌که به اینترنت متصل نیستید، بر روی صفحه شما ظاهر می‌شوند. اگر به‌طور پیوسته زیر بار صفحات تبلیغاتی قرار دارید، احتمالاً یک حشره وِبی بر روی رایانه شما نصب شده است.

✓ مرورگررُبایان

مرورگررُبایان ممکن است رایانه شما را برای استفاده خودشان به خدمت بگیرند. کاربران نرم‌افزارهای جاسوسی می‌توانند اتصال شما را برای ارسال اسپم‌ها ازطریق سرویس‌دهنده اینترنت شما، بربایند؛ به این معنی که یک اسپم‌ساز انگل می‌تواند هزاران نامه الکترونیکی اسپمی را، ازطریق اتصال رایانه شما به اینترنت و آدرس خادم اینترنت[1] شما، ارسال کند. دسترسی‌های با سرعت و حجم بالا به اینترنت اغلب هدف این نوع کاربران قرار می‌گیرد. اغلب قربانیان متوجه نمی‌شوند که از اعتبار آن‌ها سوء استفاده شده است، تا اینکه به‌خاطر شکایت علیه اسپم‌ها، سرویس‌دهنده اینترنت اتصالشان را قطع کند.

✓ مودم‌رُبایان

اگر برای اتصال به اینترنت از یک مودم و خط تلفن استفاده می‌کنید، ممکن است یک شماره‌گیر برخط برای برقراری اتصال جدید اینترنت بر روی رایانه شما نصب شود. این نرم‌افزارهای جاسوسی اغلب داخل اسپم و نامه‌های الکترونیکی مربوط به امور جنسی قرار دارند.

✓ اِسپم‌ها[2]

آیا تاکنون در ارتباط با اینترنت، نامه الکترونیکی ناخواسته دریافت کرده‌اید؟ بعضی ادعا می‌کنند که شما را به‌سرعت ثروتمند می‌کنند، برخی دیگر قول محصولات یا خدمات

1. Internet Service Provider
2. Spam

جدید را می‌دهند و بعضی صندوق پستی شما را اشغال می‌کنند و می‌خواهند که نامه الکترونیکی را برای بقیه بفرستید یا وب‌سایت مشخصی را ببینید. در جامعه اینترنتی، نامه‌های الکترونیکی ناخواسته را اسپم می‌گویند.

اسپم اثری بیش از مزاحمت برای استفاده‌کنندگان اینترنت دارد و به‌طور جدی بازدهی شبکه و سرویس‌دهندگان نامه الکترونیکی را تحت‌تأثیر قرار می‌دهد. علت اصلی این امر، هزینه بسیار پایین نامه الکترونیکی است، به همین دلیل نفوذگران صدها هزار یا حتی میلیون‌ها نامه الکترونیکی را در یک زمان ارسال می‌کنند. حمله‌های اسپم، پهنای باند زیادی را می‌گیرد؛ صندوق‌های پستی را پر می‌کند و زمان خوانندگان نامه الکترونیکی را تلف می‌کند. گاهی می‌توان اسپم‌ها را از عنوان‌های عجیب، غیرمنطقی و مضحکشان تشخیص داد.

سرقت کوکی[1]

کوکی، اطلاعاتی است که توسط وب‌سرور برای ذخیره در مرورگر ارسال می‌شود تا براساس آن وب‌سرور ارتباط قبلی کاربر را کنترل کند. کوکی، فرمت فایل متنی را دارد که در دایرکتوری مربوط به مرورگر ذخیره می‌شود و درست هنگامی که مرورگر درحال اجراست، در حافظه خواندنی و نوشتنی[2] قرار می‌گیرد. این اطلاعات می‌تواند وقتی کاربر از وب‌سایت خاصی خارج شد، در هارد درایو ذخیره شود.

مهم‌ترین استفاده از کوکی‌ها برای ذخیره شناسه و گذرواژه کاربران و کاربرد بسیار مهم دیگر آن، کنترل کاربران در صفحات آغازین است. در این حالت مقداری از هارد رایانه شما برای ذخیره این اطلاعات از مرورگرتان تقاضا می‌شود. به این ترتیب، هر زمان که به آن وب‌سایت وارد می‌شوید، مرورگر شما بررسی می‌کند که آیا

1. Cookie
2. Ram

اولویت‌های از پیش تعیین‌شده (کوکی) برای آن سرور مشخص دارید یا خیر؟ اگر این‌طور باشد، مرورگر کوکی را همراه با تقاضای شما برای صفحه وب، به وب‌سرور ارسال خواهد کرد. مایکروسافت و نت‌اسکیپ از کوکی‌هایی برای ایجاد صفحات آغازین شخصی روی وب‌سایت‌هایشان استفاده می‌کنند. استفاده‌های معمول که شرکت‌ها به‌خاطر آن‌ها از کوکی استفاده می‌کنند، شامل سیستم‌های سفارش برخط، شخصی‌سازی سایت‌ها و ردگیری وب‌سایت‌ها می‌شود.

ارتباط‌رُبایی[1]

ارتباط‌ربایی در اصل به‌معنای هواپیمارُبایی یا سایر وسایط نقلیه به‌همراه مسافران آن است. این واژه در فرهنگ نفوذگران، نوعی حمله به شبکه است که مهاجم، کنترل ارتباط را در اختیار می‌گیرد. در این حالت نفوذگر بین دو عنصر شبکه قرار گرفته و برای هرکدام از طرفین ارتباط، خود را جای دیگری معرفی می‌کند (گروه امداد امنیت رایانه ایران).

حمله به برنامه‌های تحت وب

این حمله‌ها تا حدود زیادی مبتنی بر ضعف برنامه‌نویسی است. بسیاری از برنامه‌های وب، اطلاعاتی را از کاربر می‌گیرند و پس از پردازش آن برمبنای الگوریتم‌های خود نتایجی را تولید می‌کنند. به‌عنوان مثال: برنامه یک فرم جست‌وجوی ساده را در اختیار کاربر قرار می‌دهد که عبارت «جست‌وجو» در آن وارد شده است، پس از جست‌وجو در پایگاه داده نتایجی تولید و برای کاربر نمایش داده می‌شود. این فرایند یک نمونه عملکرد بسیار رایج است که در خیلی از برنامه‌های وب مشاهده می‌شود.

اگر طراحان و برنامه‌نویسان به امور امنیتی بی‌توجه باشند، برنامه آن‌ها از همین نقطه قابل نفوذ خواهد بود. برای مثال: اگر برنامه‌نویسان به تزریق کدهای پرس‌وجوی بانک

1. Hijacking

اطلاعات آشنا نباشند، نفوذگر ممکن است بتواند با واردکردن یک عبارت جست‌وجو، ثبات و امنیت برنامه وب را به خطر بیاندازد. این خطر به حدی است که حتی اگر زیرساخت امنیتی بسیار مستحکمی ـ به‌عنوان مثال فایروالی مناسب که همه حمله‌ها را متوقف کند ـ مورد استفاده قرار گرفته باشد، ولی ورودی‌های کاربران ارزیابی نشود، تمام تلاشی که برای ایجاد زیرساخت امنیتی به‌کار رفته است، به هدر می‌رود. داده‌های نامطمئن ازطریق رشته‌های پُرس‌وجوی آدرس اینترنتی، فرم‌های «HTML»، کوکی‌ها، پرس‌وجوهایی که بر روی یک پایگاه داده انجام می‌شوند، به سامانه راه پیدا می‌کنند. رایج‌ترین حمله‌هایی که درنتیجه استفاده از داده نامطمئن بر روی برنامه و وب‌سایت صورت می‌گیرد، تزریق اسکریپت[1] و کدهای پرس‌وجوی بانک اطلاعاتی[2] است.

دزدی هویت[3]

دزدی هویت چیزی فراتر از هرزنامه‌های ناخواسته و مزاحم هستند. آن‌ها می‌توانند منجر به دزدیده‌شدن شماره‌های اعتباری، گذرواژه، اطلاعات حساب یا سایر اطلاعات شخصی کاربران شوند. دزدی هویت، فریبی طراحی شده است که برای دزدیدن هویت کاربران به‌کار می‌رود. در این نوع حمله، نفوذگر سعی می‌کند اطلاعات شخصی کاربران را، با متقاعدکردن آن‌ها به دادن این اطلاعات، تحت ادعاهای دروغین، به‌دست آورد. این نوع حمله‌ها اغلب ازطریق هرزنامه یا پنجره‌های «پایین‌افتادنی» اجرا می‌شود.

یک دزدی هویت توسط نفوذگری که هزاران نامه الکترونیکی فریبنده فرستاده است، آغاز می‌شود. به‌طوری‌که به‌نظر می‌رسد از وب‌سایت‌های معروف یا از سایت‌های مورد اعتماد مانند بانک رسیده است. این‌گونه نامه‌ها به‌قدری ماهرانه طراحی می‌شوند

1. Script Injection
2. SQL Injection
3. phishing

که بسیاری از کاربران را فریب می‌دهد. بنابراین کاربران فریب خورده و به درخواست‌های رسیده مانند اعلام شماره کارت اعتباری، گذرواژه و سایر اطلاعات شخصی پاسخ می‌دهند. نفوذگر (جاعل)، لینکی در یک نامه الکترونیکی جعلی قرار می‌دهد و این‌گونه وانمود می‌کند که لینک به وب‌سایت واقعی مرتبط است، اما با تقلب، شما را به سایتی هدایت می‌کند که دقیقاً مانند سایت اصلی است. در این حالت کاربران فریب خورده و اطلاعات شخصی خود را وارد کرده و نفوذگر از آن‌ها برای مقاصد خویش استفاده می‌کند (گروه امداد امنیت رایانه ایران).

شنود

هرگاه در اینترنت به یک اتاق گفت‌وگو وارد می‌شوید و مخاطب خود را انتخاب می‌کنید، با فعال‌سازی میکروفن، بلندگو و دوربین، به مشاهده یکدیگر و گفت‌وگو می‌پردازید؛ در این حالت احتمال دسترسی غیرمجاز نفوذگران به صوت و تصویر شما وجود دارد، اما قصه در همین‌جا پایان نمی‌یابد، اگر رایانه شما دارای میکروفن، بلندگو و دوربین باشد، احتمالاً نفوذگران منتظر شما نخواهند ماند که آن‌ها را فعال کنید و به ایشان مجوز شنود و مشاهده محل استقرار خود را بدهید، بلکه پنهانی و بدون مجوز نسبت به فعال‌سازی سامانه‌های شما اقدام کرده و از آن بهره‌برداری می‌کنند. بنابراین هرگاه شما رایانه خود را روشن می‌کنید، امکان شنود محیطی را نیز برای نفوذگران فراهم می‌سازید.[۱]

ساختار شبکه‌های اجتماعی مبتنی بر ساختار اینترنت بوده و خصوصیات کاربردی و کارکردی آن به سادگی مورد مطالعه قرار گرفته است. ساختار مسیردهی پروتکل اینترنت و پیوندهای ابرمتن وب جهان‌گستر؛ هر دو شبکه‌های مقیاس – آزاد هستند. همانند

۱. درحالتی که رایانه شما مجهز به میکروفن و دوربین است.

ارائه‌دهندگان تجاری اینترنت که ازطریق نقاط تبادل اینترنت به هم وصل می‌شوند؛ شبکه‌های پژوهشی نیز تمایل دارند بسیاری از دانشمندان علوم رایانه اینترنت را نمونه برجسته‌ای از یک سیستم بزرگ بسیار مهندسی شده و هنوز بسیار پیچیده توصیف کنند. اینترنت به‌شدت ناهمگن است، مثلاً نرخ انتقال داده و ویژگی‌های فیزیکی اتصالات بسیار تغییر می‌کند. اصول مسیریابی و آدرس‌دهی ترافیک در اینترنت به خاستگاه آن در سال ۱۹۶۰ برمی‌گردد که اندازه و محبوبیت آینده اینترنت قابل پیش‌بینی نبود؛ از این امکان ایجاد ساختارهای دیگر در دست بررسی است (صفری‌نژاد، ۱۳۹۲: ۶۸).

٤/ب. اهمیت داده‌های شبکه‌های اجتماعی

سایت‌های شبکه‌های اجتماعی منبع مهمی برای داده‌های مربوط به رفتار طبیعی کاربران هستند. اطلاعات پروفایل‌ها، پیوندهای موجود در آن‌ها، دیدگاه‌های منتشر یا مبادله‌شده، منابعی غنی برای تحلیلگران شبکه به‌شمار می‌آیند تا به الگوهای فکری، رفتاری و شاخص‌های دیگر کنشگری کاربران دست یابند. به‌عنوان نمونه؛ گُلدر[1] در سال ۲۰۰۷، مجموعه داده‌های مربوط به ۳۶۲ میلیون پیام مبادله شده، چهار میلیون و دویست هزار کاربر فیسبوک را طی ۲۶ ماه مورد بررسی و تحلیل قرار داده و به الگوی موقتی وابسته به زمان، از رفتارهای دانشجویان در این سایت شبکه اجتماعی دست یافتند (کوهی، ۱۳۹۲: ۳۳).

٥/ب. کاربران شبکه‌های اجتماعی مجازی

کاربران شبکه‌های اجتماعی می‌توانند در سایت‌ها، صفحه‌ها و پروفایل‌های شخصی برای خودشان ایجاد کنند و شبکه مجازی از دوستانشان پدید آورند. آن‌ها می‌توانند همانند فضایی که وبلاگ‌ها و میکرو وبلاگ‌ها در اختیارشان قرار می‌دهند، یادداشت‌های کوتاه و بلندشان را منتشر کنند،

1. Golder

عکس، صدا و ویدیوهای شخصی‌شان را آپلود کنند، از آخرین اخبار و رویدادها در حوزه‌های مختلف آگاه شوند و در صفحه‌های هواداری و اتاق‌های گفت‌وگوی متنوع عضو شوند و قابلیت‌های فراوان دیگری که ممکن است هر شبکه اجتماعی برای کاربرانش فراهم کند.

در اینترنت کاربرانی هم وجود دارند که در استفاده از امکانات جدید اینترنتی پیشگام هستند، ولی نسبت به عضویت در شبکه‌های اجتماعی اشتیاقی نشان نمی‌دهند و در فعالیت‌های برخط‌شان آن‌ها را به‌کار نمی‌گیرند. این نوع کاربران غیر شبکه‌های اجتماعی نیز در سه گروه قرار گرفته‌اند. آن‌ها دلیل عدم استفاده از این سایت‌ها را نداشتن وقت کافی، احساس عدم امنیت و احمقانه دانستن فعالیت در این شبکه‌ها اعلام کرده‌اند و به ترتیب «کاربران پرمشغله» «کاربران نگران» و «کاربران بدبین» نام‌گذاری شده‌اند (امیدوار طهرانی، ۱۳۹۱: ۱۵).

٦/ب. گروه سنی کاربران

در آخرین گزارشی که مرکز تحقیقاتی پیواینترنت ارائه کرده است، رشد شبکه‌های اجتماعی از سپتامبر ۲۰۰۵ تا مِی ۲۰۱۰ در بین چهار گروه سنی ۱۸ الی ۲۹؛ ۳۰ الی ۴۹؛ ۵۰ الی ۶۴؛ و بالاتر از ۶۴ سال بررسی شده است. براساس این گزارش که در ماه آگوست ۲۰۱۰ منتشر شد، استفاده از شبکه‌های اجتماعی بین کاربران ۵۰ الی ۶۴ ساله از ۲۵ درصد به ۴۷ درصد افزایش یافته است. این رقم حاکی از رشد کاربری ۸۸ درصدی این گروه سنی در شبکه‌های اجتماعی از آوریل ۲۰۰۹ تا ماه مِی ۲۰۱۰ است.

بر این اساس، حضور کاربران بالای ۶۵ سال در سرویس‌های اجتماعی چون فیسبوک و توئیتر، دو برابر شده است. به‌عبارت دقیق‌تر جمعیت ۱۳ درصدی این گروه سنی از کاربران، از ۱۳ درصد به ۲۶ درصد افزایش یافته است؛ این درحالی است که رشد پایگاه کاربری

افراد ۱۸ الی ۲۹ ساله طی دوره مذکور از ۷۶ درصد به ۸۶ درصد رسیده است، درحالی که رشد کاربران ۱۸ الی ۲۹ ساله در سال ۲۰۰۷ به ۶۷ درصد افزایش یافته بود، استقبال از شبکه‌های اجتماعی به‌تدریج در بین کاربران میانسال و سالخورده افزایش یافت. برای مثال در ماه می ۲۰۰۸ این گروه سنی فقط حدود ۲۵ درصد از جمعیت کاربران شبکه‌های اجتماعی را تشکیل می‌داد و گروه سنی ۵۰ الی ۶۴ ساله هم تنها ۱۱ درصد کل کاربران شبکه‌های اجتماعی را شامل می‌شد، این درحالی است که جمعیت کاربران بالای ۶۵ سال فقط به ۷ درصد می‌رسید. بااین‌حال از آن زمان تا کنون نرخ رشد گروه‌های سنی سالخورده‌تر نسبت به گروه سنی ۱۸ الی ۲۹ ساله سریع‌تر بوده است.

مری مدن (یکی از متخصصان ارشد تحقیق مرکز تحقیقاتی Pew) می‌گوید: درحالی که کاربران بزرگسال جوان، وزنه اصلی شبکه‌های اجتماعی به حساب می‌آیند، رشد جمعیت این پایگاه کاربری در مقایسه با گروه‌های سنی بالاتر، کمتر بوده است.

به‌عبارت دیگر در بین هر ۵ نفر کاربر برخط ۵۰ تا ۶۴ ساله، یک نفر هر روز در شبکه‌های اجتماعی به فعالیت می‌پردازد. همچنین نرخ رشد کاربری افراد بالای ۶۵ سال در سال ۲۰۱۰ به ۱۳ درصد می‌رسد که این رقم در سال ۲۰۰۹ فقط ۴ درصد بوده است (امیدوار طهرانی، ۱۳۹۱: ۳۸).

۷/ب. ضریب نفوذ اینترنت

جدول ۱: ضریب نفوذ اینترنت به تفکیک سال در کشور (http://www.ircert.com)

۱۳۹٤	۱۳۹۳	۱۳۹۲	۱۳۹۱	۱۳۹۰
۸۲/۱۲	۷۳/۹٤	۷۹/۱۳	٦۱/۰٦	٤۳/۲۳

جدول ۲: ضریب نفوذ اینترنت به تفکیک فناوری (همان)

۱۳۹۳					۱۳۹٤				
Mobil	Wimax	Fiber	Dialup	ADSL	Mobil	Wimax	Fiber	Dialup	ADSL
۲۳.۹۹	۴.۲۷	۸.۲۵	۶.۷۵	۲۷.۷۱	۲۷.۵۲	۴.۱۷	۸.۲۵	۶.۷۵	۳۰.۳۹

جدول ۳: تعداد مشترکین اینترنت به تفکیک سال (همان)

۱۳۹۰	۱۳۹۱	۱۳۹۲	۱۳۹۳	۱۳۹۴
۱۹۹۲۱۲۳۷	۳۲۸۳۸۶۱۹	۲۱۱۹۸۹۴۵	۳۷۴۸۴۰۷۷	۴۳۰۲۶۲۷۹

۸/ب. شبکه‌های اجتماعی مجازی و تهدیدهای نوین

شبکه‌های اجتماعی مجازی یکی از نشانگاه‌های جنگ سایبری می‌باشند. شبکه‌های اجتماعی مجازی، نوعی فناوری‌های رایانه‌ای بوده که جدایی از نسل اول وب برمبنای اصل دوم وب یا ابتکار وب۲ ساخته شده‌اند. وب۲ اشاره به سامانه‌ای دارد که بارگذاری محتوایی آن شامل اطلاعات و داده‌ها به هر شکل به عهده کاربران است. شبکه‌های اجتماعی مجازی یک شبکه تار عنکبوتی با میلیاردها پیوند است که با اضافه‌شدن امکاناتی همانند: چت، ایمیل و چیزهای دیگر، این امکان را به کاربران خود می‌دهد که ازطریق به اشتراک‌گذاری؛ اطلاعات و داده‌های خود را در اختیار سایرین قرار دهند.

شبکه‌های اجتماعی مجازی فارغ از مرز، زبان، جنس، نژاد، فرهنگ و...، محل گردهمایی صدها میلیون کاربر اینترنتی است. یک شبکه اجتماعی در مرحله اول به افراد اجازه می‌دهد صفحات دلخواهشان را روی آن ایجاد کنند و در مرحله دوم این صفحات براساس مشترکات گوناگون به هم وصل می‌شوند و کاربران می‌توانند به‌طور مشترک از اطلاعات و داده‌های یکدیگر بهره‌مند شوند. تأثیرات این شبکه‌ها تا آنجاست که در برخی مواقع اقدام‌های خود را به فضای واقعی جامعه نیز تسرّی داده و باعث هماهنگی و

سازماندهی بسیاری از تجمع‌های سیاسی و اعتراضی می‌شوند؛ به‌نحوی که امنیت ملی را در حوزه‌های گوناگون تهدید می‌نمایند. در هر صورت شبکه‌های اجتماعی مجالی برای شکل‌گیری اجتماع‌های جدیدی از کاربران فراهم می‌کنند (ضیایی‌پرور، ۱۳۷۸: ۱۵).

۹/ب. برخی از شبکه‌های اجتماعی مجازی فعال

جدول ۴: شبکه‌های اجتماعی مجازی (شکیب، ۱۳۹۲: ۲۱۸)

ردیف	نام شبکه	آدرس	محتوا
۱	یوتیوپ	YOUTUBE.COM	محتوامحور- تصاویر ویدئویی
۲	فلیکر	Fliker.COM	محتوامحور- عکس
۳	پیکاسا	Picasaweb.google.com	محتوامحور - عکس
۴	تامبلر	Tumblr.com	محتوامحور- عکس
۵	ساوند کلود	Soundcluod.com	محتوامحور- فایل‌های صوتی و موسیقی
۶	ویکی‌پدیا	Wikipedia.com	محتوامحور- مدخل دانشنامه همگانی
۷	دلیشز	Delicious.com	محتوامحور-لینک مطالب سایت‌ها و وبلاگ‌ها
۸	گوگل ریدر	Reader.google.com	محتوامحور- محتوای موجود در همه سایت‌ها و وبلاگ‌ها
۹	بالاترین	Balatarin.com	محتوامحور- لینک خلاصه مطالب در همه سایت‌ها
۱۰	گوگل ارت	Earth.google.com	محتوامحور- اطلاعات زمین
۱۱	گودریدز	Goodreads.com	محتوامحور- کتب مورد علاقه
۱۲	توئیتر	Twitter.com	کاربرمحور- تک محتوایی
۱۳	فیسبوک	Facebook.com	کاربرمحور- چندمحتوایی
۱۴	فرندفید	Friendfeed.com	کاربرمحور- چندمحتوایی
۱۵	گوگل باز	Google.com/buzz	کاربرمحور- چندمحتوایی
۱۶	سوپ	Soup.io	کاربرمحور- چندمحتوایی
۱۷	مای اسپیس	Myspsce.com	کاربرمحور- چندمحتوایی
۱۸	اور کات	Orkut.com	کاربرمحور- چندمحتوایی
۱۹	تلگرام	telegram.com	کاربرمحور- چندمحتوایی
۲۰	اسکیپ	eskip.com	کاربرمحور- چندمحتوایی

۱۰/ب. برخی از شبکه‌های اجتماعی فعال خارجی و ایرانی

دو جدول زیر به‌صورتی خلاصه اعداد و ارقام مربوط به استفاده از دو نوع از شبکه‌های اجتماعی ایرانی و رقبای خارجی‌شان را مرور می‌کند.

جدول ۵: برخی از شبکه‌های اجتماعی فعال خارجی

توئیتر تولد: ۲۰۰۶ جمعیت: ۶۰۰ میلیون نفر تعداد کاربران ایرانی: کمتر از یک میلیون نفر زادگاه: امریکا	**تلگرام** تولد: ۲۰۱۳ جمعیت: حدود ۵۰ میلیون نفر زادگاه: روسیه
اینستاگرام تولد: ۲۰۱۱ جمعیت: ۴۲۰ میلیون نفر تعداد کاربران ایرانی: حدود چهار میلیون نفر زادگاه: امریکا	**فیسبوک** تولد: ۲۰۰۴ جمعیت: ۱۴۰۰ میلیون نفر تعداد کاربران ایرانی (غیررسمی): بیش از ۱۰ میلیون نفر زادگاه: امریکا

جدول ۶: برخی از شبکه‌های اجتماعی فعال ایرانی

آپارات تولد: ۱۳۸۹ جمعیت: بیش از ۵۰۵ هزار نفر جهانی	**فیس‌نما** تولد: ۱۳۹۰ جمعیت: بیش از یک میلیون و صدهزار نفر
کلوب تولد: ۱۳۸۳ جمعیت: دو میلیون و ۸۰۰ هزار نفر (http://www.ircert.com)	

جدول ۷: اندیشه‌های بنیادین شبکه‌های اجتماعی (شکیب، ۲۱۸:۱۳۹۲)

ردیف	عنوان	توضیح
۱	نظارت	نظارت دائمی، درونی‌شدن رفتار مطابق میل شبکه
۲	جهان دوم	جهانی ذهنی موازی با جهان واقعی، مانند فیلم ماتریکس یا آواتار
۳	دهکده جهانی	محل تجمع و یافتن همه مردمان جهان به‌خصوص هم‌زبانان و دوستان
۴	فرهنگ واحد جهانی	اشغال ذهن‌ها به‌جای اشغال سرزمین‌ها یا حکومت‌ها
۵	دموکراسی	رأی‌گیری برای سنجش هر موضوعی مانند حقایق تاریخی
۶	لیبرالیسم	آزادی مطلق و بدون نظارت، منتج به انحصارطلبی
۷	نظام مشارکت جمعی	تولیدات رسانه‌ای توسط شهروندان عادی، روزنامه‌نگاری شهروندی
۸	جامعه شبکه‌ای	جماعت برخط
۹	روابط آزاد اجتماعی	برقراری رابطه با هرکسی و در هر زمانی بدون هیچ نظارتی
۱۰	میل به دیده‌شدن	ایجاد فرصت ابراز وجود و خودنمایی به افراد عادی
۱۱	حوزه عمومی	فضای آزاد جهت طرح موضوع‌های جامعه

۱۱/ب. ایران و شبکه‌های اجتماعی و کارکردهای آن

شمار کاربران اینترنتی در ایران در سال ۱۹۴۴ از ۲۵۰ نفر فراتر نمی‌رفت، اکنون براساس جدیدترین آمارها بالغ بر ۱۲ میلیون نفر به شبکه جهانی اینترنت متصل هستند (جمعی از نویسندگان، ۱۳۸۸: ۱۵۹). شبکه‌های اجتماعی مجازی که محصول گسترش فناوری‌های نوین ارتباطی هستند، در ایران با استقبال چشمگیری روبه‌رو شده‌اند. برای اولین بار نام ایرانی‌ها در رتبه‌بندی فناوری‌های اینترنتی به نام وبلاگ عجین شد. ایرانی‌ها توانستند در سال ۱۳۸۳ و ۱۳۸۴ رتبه چهارم وبلاگ‌نویسی را به خود اختصاص دهند.

اکنون می‌توان تخمین زد حدود شش میلیون وبلاگ فارسی در فضای اینترنت ثبت شده و به جرئت می‌توان گفت وبلاگستان فارسی یکی از بزرگ‌ترین شبکه‌های اجتماعی ایرانیان است. در بین وبلاگ‌های ثبت شده خارجی، وبلاگ اورکات مورد استقبال ایرانیان قرار گرفت، اما پس از فیلترینگ این شبکه، کلوب ادعا می‌کند بزرگ‌ترین جامعه مجازی ایرانیان را در اختیار دارد (ضیایی‌پرور، ۱۳۸۸: ۱۳).

آنچه که در این بخش مورد توجه است دلایل استقبال ایرانیان از شبکه‌های اجتماعی است. به‌طور خلاصه این مهم را می‌توان از ابعاد مختلف مورد بحث و بررسی قرار داد.

جدول ۸: دلایل استقبال کاربران ایرانی از شبکه‌های اجتماعی

ردیف	ابعاد	ملاحظات
۱	فنی	رفع فیلتر شبکه‌های اجتماعی، امکانات فوق‌العاده، ناتوانی دولت در رصد آن‌ها
۲	سیاسی	ناتوانی در انجام مشارکت حقیقی و روی‌آوردن به مشارکت مجازی
۳	اجتماعی	مزیت فعالیت‌های شبکه‌ای و دشواری اختلال در روند این‌گونه فعالیت‌ها
۴	فرهنگی	سرگرم‌شدن، مُدگرایی، کنجکاوی در اطلاعات دیگران
۵	روان‌شناختی	میل به برقراری ارتباط و دیده‌شدن
۶	رسانه‌ای	خلأ پوششی برخی از موضوع‌ها در دیگر رسانه‌ها و پاسخگویی به آن‌ها در این‌گونه شبکه‌ها

۱۲/ب. تهدیدها و چالش‌های شبکه‌های اجتماعی

با گسترش روزافزون شبکه‌های اجتماعی در ایران، تهدیدگران فضای امنیتی جامعه، با سوء استفاده از فرصت فراهم شده توسط این شبکه‌ها، به مقابله با نظام اسلامی پرداختند. این اتفاق، شبکه‌های اجتماعی را به تهدیدی برای امنیت اطلاعات تبدیل نمود، به‌طوری که نام این شبکه‌ها با جنبش سبز، انقلاب توئیتری و اطلاع‌رسانی سریع، عجین گشت. هرچند که بسیاری از کشورهای غربی با استفاده از این شبکه‌های اجتماعی و فضای مجازی در صدد تهدید فضای امنیتی جامعه ما هستند، ولی خود نیز از آسیب‌های آن در امان نبوده و با مسائل متعددی ازقبیل امنیت روانی کودکان و نوجوانان، نقض حریم خصوصی و امنیت اطلاعات دست به گریبان هستند. تهدیدها و چالش‌های شبکه‌های اجتماعی حوزه‌های گوناگونی را دربر می‌گیرد، ازجمله: حوزه سیاسی ــ امنیتی، حوزه فرهنگی اجتماعی و حوزه اقتصادی. در اینجا به اختصار هریک از حوزه‌ها را در قالب جداول زیر بررسی خواهیم کرد.

جدول ۹: حوزه سیاسی و امنیتی (گزارش راهبردی رسانه ۱۰، ۱۳۸۹: ۴۵)

۱	مدیریت غرب‌گرایانه و قوانین دوگانه	خدمت‌رسانی به تهدیدگران نظام، اعمال محدودیت برای مدافعان نظام
۲	کنترل افراد و جاسوسی	استفاده از اطلاعات خصوصی کاربران در جهت منافع خود، جاسوسی از آن‌ها
۳	کنترل جامعه و سنجش افکار عمومی	به‌دست آوردن برآیند نظرهای کاربران در مورد موضوع‌های مختلف، نظرسنجی پنهانی
۴	سوپاپ اطمینان و تسکین هیجانی	القای انجام وظیفه به افراد، تبدیل فعالیت واقعی به مجازی و بی‌خطر
۵	توهم سیاسی، حذف دگراندیشان	ایجاد حس بی‌شمار بودن در کاربران، خاموش کردن صدای مخالفان
۶	انتشار محتوای غیر رسمی و اسناد محرمانه	انتشار اطلاعات مهم به‌صورت غیر رسمی به‌منظور تأثیرگذاری
۷	افزایش امکانات گروهک‌های معارض	ایجاد امکان ارتباط امن و پنهان برای گروهک‌ها و سازماندهی فعالیت‌های آن‌ها
۸	عبور از سد مسدودسازی و فیلترینگ	عدم امکان فیلترینگ شبکه‌های اجتماعی، عبور از فیلترینگ به‌وسیله شبکه‌های اجتماعی
۹	دیپلماسی سایبر، دیپلماسی شبکه‌های اجتماعی	شبکه‌های اجتماعی به‌مثابه پنجره‌ای رو به ایران و جامعه ایرانی
۱۰	امنیت سایبری	سلب آزادی بیان به بهانه تأمین امنیت، واکنش شدید در برابر مخالفت‌ها

جدول ۱۰: حوزه فرهنگی و اجتماعی

۱	گسترش عناصر و ارزش‌های بنیادین غربی	تغییر تدریجی جهان‌بینی و هویت کاربران به‌دلیل سیر طولانی‌مدت در فضایی فرهنگی متعلق به غرب
۲	تغییر عادت‌ها، اعتیاد سایبری	ایجاد عادت‌های نامطلوب در کاربران، اعتیاد آن‌ها به شبکه‌های اجتماعی
۳	فرهنگ نامطبوع حاکم بر شبکه	کثرت خلقیات منفی در فرهنگ مجازی کاربران، عدم تحمل یکدیگر
۴	ترویج ادیان مخدوش	تشکیک و تخریب دین، جایگزینی عرفان‌های دروغین و ادیان شخصی‌شده
۵	روابط اجتماعی فراتر از چارچوب اسلامی	عدم پایبندی به احکام دین در دنیای مجازی
۶	محتوای ضد اخلاقی و نامناسب	دسترسی آسان به محتوای ضد اخلاقی، عدم تناسب با انسان ایرانی
۷	اطلاعات بی‌فایده و نادرست	پرکردن اذهان کاربران از اطلاعات بی‌فایده، آگاهی کاذب به‌عنوان یکی از شیوه‌های جنگ نرم
۸	سرگرمی محوری	تولید محتوای بی‌فایده تنها برای ایجاد رابطه، شبکه‌های اجتماعی به‌مثابه وسیله اوقات فراغت
۹	پارادوکس سرمایه اجتماعی، کاهش آن	کاهش سرمایه اجتماعی با منفعل کردن کاربران و از بین بردن عناصر کلیدی هویت آن‌ها

جدول ۱۱: حوزه اقتصادی و مالی

۱	مالکیت غربی، استقرار در امریکا	شبکه‌های معروف در مالکیت مالکان امریکایی قرار دارند و دفتر مرکزی آن‌ها در امریکا مستقر است
۲	منابع درآمدی نامشروع	فروش اطلاعات کاربران به دولت‌ها، سازمان‌های جاسوسی و شرکت‌ها
		تبلیغات، حمایت از شبکه‌های تهدیدگر با واگذاری تبلیغات به آن‌ها
		پول مجازی، تهییج کاربران به سرمایه‌گذاری به‌وسیله پول واقعی در یک بازی مجازی
		اجازه جست‌وجو در اطلاعات به موتورهای جست‌وجوگر، تبدیل شبکه‌های اجتماعی به منابع دانشی
۳	سوء استفاده از خدمات کاربران	تماشای تبلیغات، بالابردن اعتبار شبکه با فعالیت در آن، شرکت ناآگاهانه در تحقیقات به‌مانند موش آزمایشگاهی
۴	تقویت نظام سرمایه‌داری	روانه ساختن منابع درآمدی عظیم به حساب سرمایه‌داران صهیونیست، تغییر عادت‌های کاربران در جهت درآمدزایی
۵	کاهش بهره‌وری	اختلال در تمرکز کارمندان و دانشجویان و کاهش بهره‌وری در فعالیت آن‌ها، ایجاد آسیب اقتصادی
۶	تسهیل فعالیت شرکت‌های هرمی	ترویج شرکت‌های هرمی در شبکه‌های اجتماعی

۱۳/ب. روش‌ها و فنون رسانه‌ای شبکه‌های اجتماعی با هدف تهدید امنیت اطلاعات

فنون رسانه‌ای، روش‌هایی هستند که در مراحل حساس توسط رسانه‌ها به‌کار گرفته می‌شود تا توان اندیشیدن، تصمیم‌گیری و اقدام به‌موقع را از جامعه هدف گرفته و امکان دستیابی به هدف‌های نبرد در فضای مجازی را افزایش دهند. فنون رسانه‌ای به‌طور کلی به دو دسته تاکتیک‌های اصلی و واسطه‌ای تقسیم می‌شوند. بدین ترتیب که تاکتیک‌های واسطه‌ای اغلب به‌عنوان وسیله‌ای برای اجرای تاکتیک‌های اصلی به‌کار می‌روند. تاکتیک‌های اصلی هم در صورت موفقیت، عرصه را برای اقدام‌های تهدیدآمیز بازیگران جنگ نرم مهیا می‌کنند.

جدول ۱۲: تاکتیک‌های رسانه‌ای در فضای شبکه‌های اجتماعی (گزارش راهبردی رسانه ۱۹، ۱۳۸۹: ۱۰)

تاکتیک اصلی	تردیدافکنی
	ایجاد فضایی پر از هیجان
	ایجاد اختلاف
	فریب
	از بین بردن نقاط قوت
تاکتیک واسطه‌ای	برجسته‌سازی
	اتهام‌زنی
	انگ زدن، برچسب زدن
	شایعه
	توسل به طنز
	مغالطه و دروغ‌گویی
	پیوندزدن
	ترور شخصیت و شخصیت‌سازی کاذب
	پاره حقیقت‌گویی
	تحریف
	ترور تصویری
	ترس و وحشت

۱۴/ب. کارکرد شبکه‌های اجتماعی در مراحل مختلف جنگ نرم

شرایط عادی

- تأثیرگذاری بر افکار عمومی ازطریق کسب اعتماد و متقاعدسازی به‌عنوان یک فناوری بی‌طرف؛
- اشاعه فرهنگ غربی و ترویج بی بند و باری، انتشار محتوای ضد اخلاقی؛
- انتشار اخبار غیر رسمی در حوزه‌های امنیتی سیاسی؛
- ترویج روحیه کم‌کاری و ترویج فسادهای اقتصادی از جمله تشویق در جهت عضویت در شرکت‌های هرمی.

آستانه بحران

- نبردهای تبلیغاتی ازطریق گسترش عقاید مخالفان؛
- برجسته‌سازی برخی از اخبار سیاسی؛
- سنجش دروغین افکار عمومی.

حین بحران

- انتشار اخبار و بیانیه‌های مخالفان؛
- نمادسازی و اسطوره‌سازی، افکارسازی؛
- تبدیل‌شدن به اتاق فکری مجازی و تغذیه فکری مخالفان و متقاعدسازی آن‌ها؛
- آموزش اقدام‌های خشونت‌بار (مانند روش‌های ساخت انواع بمب و...) و غیرخشونت‌بار؛
- استفاده از پدیده خبرنگار شهروند به‌معنی دریافت اطلاعات و داده‌های شهروندان و مخالفان شامل: عکس، تصویر، کلیپ، موسیقی، کاریکاتور و... و به اشتراک‌گذاری آن برای سایر کاربران به‌منظور ارائه چهره مخدوشی از نظام سیاسی؛
- هدایت‌سازی و سازماندهی مخالفان داخل و خارج در فضای سایبر.

پس از بحران

پس از بحران دست‌اندرکاران جنگ نرم به بازنگری در عملکرد خود می‌پردازند. بنابراین آرشیو کاملی از همه جریان‌های رخ داده را تهیه کرده و آن را در اختیار نهادهای امنیتی و پژوهشی قرار می‌دهند (شکیب، ۱۳۹۲: ۲۰۹).

۱۵/ب. مهم‌ترین آسیب‌های شبکه‌های اجتماعی از دیدگاه امنیتی:

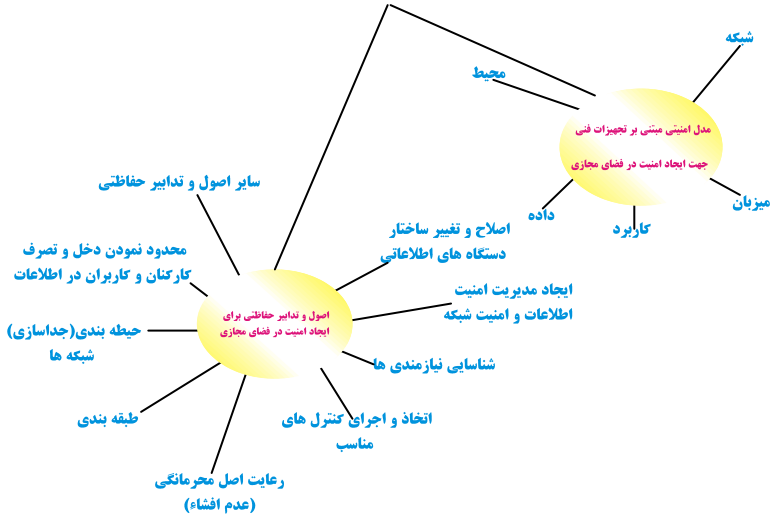
- تأثیر افکار عمومی و بسیج آن‌ها برای اغتشاش در درون کشورها؛
- تضاد با ارزش‌ها و باورها؛

- افزایش تعارض‌های ساختاری و دوگانگی هویت؛
- یکسان‌سازی فرهنگی؛
- اختلال در روند و وحدت ملی؛
- ایجاد اختلاف و شکاف میان ملت‌ها به‌دلیل ملی‌گرایی افراطی (مثل جدایی قومیت‌ها از قبیل: لرها، کردها، عرب‌ها و... مبنی بر اینکه استقلال جدا بخواهند)؛
- ایجاد نخبگان سیاسی و فرهنگی وابسته (پایگاه اینترنتی جنگ نرم)؛
- نظریه‌های متضاد و بروز شکاف فرهنگی؛
- یکپارچگی افقی گروه‌ها و طبقات و تشدید دو قطبی بودن؛
- بهره‌برداری تبلیغاتی و انتشار اخبار غیرواقعی تحریف‌شده؛
- تضعیف پیوندهای سنتی ازطریق تقویت و تبلیغ ارزش‌های بیگانه (اسدپور، ۱۳۹۲: ۲۰).

بررسی‌های به عمل آمده بیانگر آن است که بهترین دیوارهای آتش و ضدویروس‌ها با بهترین وضعیت تنها ۳۰٪ امنیت برای اطلاعات در فضای مجازی ایجاد می‌نماید (گزارش ارائه شده در نمایشگاه Cebitu ۲۰۰۴، هانوفر آلمان)، بنابراین تنها با تکیه بر سیستم‌های امنیتی مبتنی بر فناوری فنی (نرم‌افزار و سخت‌افزار) در بهترین حالت، حداکثر ۳۰٪ امنیت اطلاعات در فضای مجازی تأمین می‌گردد، لذا باید تدابیر امنیتی و حفاظتی غیر فناورانه، درون‌سازمانی به‌طور جدی مورد توجه قرار بگیرد. برای نمونه اگر بهترین سیستم رمزنگاری هم انتخاب و اجرا گردد، اما سهل‌انگاری و بی‌توجهی یک کارمند یا کاربر، می‌تواند باعث افشای کلید رمز و در نتیجه، از بین رفتن تأثیر امنیتی گردد.

از طرفی مهاجمان به سرعت نقاط ضعف فناوری‌های امنیتی را پیدا می‌کنند و یا آن‌هایی که فناوری‌های امنیتی را ارائه می‌کنند، ضعف‌های آن‌ها را می‌شناسند و ممکن است این ضعف‌ها افشا گردد و... .

الگوی امنیتی مدنظر در دو بخش، یکی اصول و تدابیر اساسی حفاظتی و دیگری مدل امنیتی مبتنی بر فناوری که مکمل یکدیگر می‌باشند ارائه می گردد. در بخش اصول و تدابیر حفاظتی، مواردی شامل اصلاح و تغییرات ساختار سنتی، ایجاد سیستم مدیریت امنیت اطلاعات در فضای مجازی و مدیریت امنیت شبکه، شناسایی و تعیین نیازمندی‌های امنیتی، سیاست کنترلی، طبقه‌بندی اطلاعات، حیطه‌بندی در شبکه‌ها، اصل محدود نمودن دخل و تصرف کارکنان و کاربران در اطلاعات و سایر تدابیر حفاظتی به‌عنوان اصول و تدابیر حفاظتی اساسی برای امنیت اطلاعات در فضای مجازی معرفی و تشریح می گردد و در بخش مدل امنیتی بر فناوری؛ پنج سطح (لایه) امنیتی و مکانیزم و فناوری‌های مؤثر در هر سطح امنیتی، معرفی و تشریح می‌شوند.



شکل ۱: الگوی امنیت اطلاعات در فضای مجازی

تجزیه و تحلیل (پاسخ به سؤال اصلی)

وجود امکانات فراوان در فضای مجازی «اینترنت» مانند: وب‌سایت‌ها، وبلاگ‌ها، مبادله فایل، گفت‌وگو، گروه‌های خبری، کنفرانس راه دور، تلفن اینترنتی، امور تجاری و... نیاز به این رسانه را الزامی کرده و آن را به یک فرصت تبدیل کرده است.

الزام به استفاده از اینترنت و شبکه‌های اجتماعی و اینکه این پدیده یک فرصت مناسب برای رشد، تبادل افکار و توسعه دانش است، واقعیت دارد، اما تهدیدهای آن نیز واقعی است.

اینترنت و شبکه‌های اجتماعی زمانی به‌عنوان یک فرصت برای توسعه دانش محسوب خواهد شد که ما با شناخت کامل و با برنامه مشخص و با درک تهدیدها به سراغ آن برویم.

نتیجه‌گیری

باتوجه به بررسی‌های انجام شده، هیچ‌گاه نمی‌توان برای اطلاعات در بستر اینترنت و شبکه‌های اطلاع‌رسانی، امنیت کامل ایجاد نمود و رایانه متصل به اینترنت برای مبادله، ذخیره‌سازی و سرور اطلاعات طبقه‌بندی شده، مناسب نمی‌باشد، اما با اتخاذ تدابیر حفاظتی و بهره‌گیری از تجهیزات فنی در این حوزه می‌توان امنیت قابل قبولی را فراهم نمود که الگوی امنیتی ارائه شده نیز با همین نگرش تهیه شده و از دو بخش مدل امنیتی مبتنی بر تجهیزات فنی و اصول و تدابیر حفاظتی تشکیل گردیده است.

یکی از راهکارهای مهم و حائز اهمیت برای امنیت اطلاعات در بستر اینترنت که در الگوی ارائه شده نیز ذکر گردیده است، حیطه‌بندی (جداسازی) شبکه‌ها می‌باشد. یعنی از اینترنت و شبکه‌های اطلاع‌رسانی می‌توان با جداسازی شبکه‌ها و براساس طبقه‌بندی اطلاعات، استفاده نمود. به‌عنوان نمونه برای اطلاعات طبقه‌بندی شده (محرمانه) از شبکه

سازمانی استفاده کرد و در نهایت اینکه اینترنت برای تبادل اطلاعات دارای طبقه‌بندی نباید مورد استفاده قرار گیرد، زیرا امنیت ندارد.

پیشنهادها و راهکارهای کاربردی برای توسعه امنیت نرم در فضای سایبر با تأکید بر شبکه‌های اجتماعی مجازی

برای استفاده از اینترنت و شبکه‌های اجتماعی به‌ویژه در حوزه دانش و پژوهش‌های طبقه‌بندی شده، باید با تهدیدها و راهکارهای پیشگیری و مقابله با آن آشنا شویم. آگاهی از مقررات و اجرای آن‌ها درست‌ترین اقدام برای استفاده صحیح از اینترنت است. بنابراین پیشنهاد می‌شود کاربران از مقررات حاکم در این حوزه مطلع گردیده و ملزم به اجرای آن شوند.

باتوجه به اینکه ارتباط ازطریق شبکه‌های اجتماعی از بستر اینترنت میسر می‌باشد، به‌عنوان یک کاربر ساده، با درک مناسب از تهدیدها و فرصت‌ها، به توصیه‌های حفاظتی توجه داشته و عمل کنیم. برخی از مهم‌ترین توصیه‌ها عبارت‌اند از:

- قبل از ارتباط با اینترنت مطمئن شوید که بر روی رایانه مورد استفاده، به هیچ عنوان اطلاعات باارزش وجود ندارد. اطلاعات طبقه‌بندی شده، عکس‌ها و فیلم‌های اداری و خانوادگی و خصوصی، یادداشت‌ها و اطلاعات خصوصی و... از جمله اطلاعاتی است که نباید بر روی رایانه شما به هنگام ارتباط با اینترنت وجود داشته باشد؛
- توصیه جدی می‌شود از رایانه جدید استفاده کنید یا اگر از رایانه قدیمی استفاده می‌کنید، تمامی اطلاعات آن را به‌صورت غیرقابل بازیافت نابود کرده و برای حصول اطمینان با استفاده از ابزارهای بازیابی آن را کنترل کنید و مطمئن شوید که به هیچ عنوان اطلاعات ارزشمند روی رایانه وجود نداشته یا قابل بازیافت نیست؛

- اگر به اینترنت متصل شده‌اید، از این به بعد این رایانه یا گوشی استفاده‌شده، قابل اعتماد نیست و این بی‌اعتمادی محدود به هنگام ارتباط با اینترنت نخواهد بود، بلکه در حالتی که به اینترنت هم متصل نیستید نباید به آن اعتماد کنید. باید بپذیرید که احتمالاً در رایانه یا گوشی که از آن برای ارتباط با اینترنت استفاده می‌کنید، نفوذ شده و انواع و اقسام ابزارهای جاسوسی در آن نصب و فعال است؛
- نباید به هیچ عنوان حتی زمانی‌که به اینترنت متصل نیستید، از رایانه یا گوشی موصوف برای امور باارزش و مشاهده اطلاعات محرمانه استفاده کنید. چون در این حالت، جاسوس‌افزارها از اطلاعات باارزش شما نسخه‌برداری، عکس‌برداری یا فیلم‌برداری کرده و ضمن کُد کردن، برای نفوذگر ذخیره می‌کنند؛
- ضروری است تجهیزات جانبی مانند فلاپی، سی.دی، دی.وی.دی، پورت یو.اس.بی، میکروفون، دوربین وب و... را کنترل کنید و مراقب سرقت اطلاعات باشید؛
- هیچ‌گاه حافظه‌های جانبی حاوی اطلاعات باارزش را به این‌گونه رایانه‌ها یا گوشی متصل نکنید؛
- به هنگام اتصال حافظه‌های جانبی به این‌گونه رایانه‌ها یا گوشی و قبل از اتصال به سایر رایانه‌ها یا گوشی‌ها، آن‌ها را توسط ضد ویروس مناسب و قابل اعتماد بررسی کنید؛
- هیچ‌گاه بر روی ایستگاه کاربری اینترنت مبادرت به نوشتن و تولید اطلاعات باارزش نکنید؛
- هیچ‌گاه بر روی ایستگاه کاربری اینترنت مبادرت به خواندن و نگاه‌کردن اطلاعات باارزش نکنید؛
- میکروفون و دوربین وب را به‌طور فیزیکی از رایانه قطع کنید و به هیچ عنوان در محیط ایستگاه کاربری اینترنت، مطالب طبقه‌بندی شده را بازگو نکنید؛
- پیکربندی امن سیستم عامل یکی از اقدام‌های مؤثر برای پیشگیری و مقابله با تهدیدهای اینترنت است؛

- به‌طور منظم و روزانه، هفتگی و ماهیانه ایستگاه کاربری را ارزیابی امنیتی کنید. این ارزیابی باید به‌صورت محلی و براساس وارسی‌نامه مناسب انجام شود؛
- هیچ‌گاه احتمال نفوذ به ایستگاه کاربری خود را منتفی ندانید و همواره بر این باور باشید که احتمالاً در رایانه شما نفوذ شده است؛
- از ورود بدافزارها جلوگیری و با آن‌ها مقابله کنید. برای این کار حتماً از آنتی‌ویروس مصوب استفاده کرده و آن را همواره به‌روزرسانی کنید؛
- نسبت به فعال‌کردن دیواره آتش سیستم عامل اقدام کنید. توصیه می‌شود به‌منظور حفاظت از ایستگاه کاربری دیواره آتش، نرم‌افزار مربوط به سیستم عامل را فعال کنید (پورمراد، ۱۳۸۹).

راهکارهای مقابله با تهدیدهای شبکه‌های اجتماعی مجازی

- بومی‌سازی شبکه‌های اجتماعی مجازی و سازماندهی و هدایت آن‌ها؛
- ارتقای سواد رسانه‌ای مخاطبان فضای مجازی به‌منظور استفاده بهینه و سودمند از این فضا ازطریق سیاستگذاری‌های فرهنگی و آموزشی در مدارس و دانشگاه‌ها و مراکز علمی و آموزشی؛
- تأکید بر تمدن اسلامی - ایرانی در فضای مجازی به‌منظور بازتولید فرهنگ اسلامی ـ ایرانی ازطریق راه‌اندازی یک نهضت وبلاگی؛
- ریشه‌یابی و آسیب‌شناسی اجتماعی، سیاسی دقیق شبکه‌های اجتماعی مجازی، مدیریت عقلانی و کنترل‌های پیشگیرانه، رصد اطلاعاتی شبکه‌های اجتماعی تهدیدمحور و فراهم‌ساختن زیرساخت‌های لازم و کافی در کنار نظارت و جهت‌دهی صحیح جایگاه رسانه‌ای جدید در عرصه اطلاع‌رسانی کشور؛
- بازاندیشی قوانین کیفری و جرائم رایانه‌ای مرتبط به این حوزه به‌دلیل تنوع روزافزون و روش‌های مخرب مورد استفاده در فضای مجازی (شکیب، ۱۳۹۲: ۲۱۲).

منابع

- اسدپور، مسعود (۱۳۹۲)، «کشف شبکه‌های پنهان کاربران فارسی»، تهران: دانشگاه امام حسین(ع).
- امیدوار طهرانی، بهروز (۱۳۹۱) «تحلیل و طراحی یک شبکه اجتماعی بومی‌شده معناگر»، پایان‌نامه دانشجویی در رشته مهندسی فناوری اطلاعات، تهران.
- پورمراد، مجید (۱۳۸۸)، «حفاظت فناوری اطلاعات»، تهران: حدیث کوثر.
- پورمراد، مجید (۱۳۸۹)، «امنیت دانش در فضای اینترنت»، فصلنامه دانش حفاظتی و امنیتی، شماره ۱۷، تهران: حدیث کوثر.
- جمال پور، حسین (۱۳۸۴)، «معماری اینترنت»، تهران: جلوه.
- چلبی، مسعود (۱۳۷۵)، «جامعه‌شناسی نظم»، تهران: نی.
- دفتر مطالعات و برنامه‌ریزی رسانه‌ها (۱۳۸۸)، «شبکه‌های اجتماعی»، گزارش راهبردی رسانه ۲، تهران.
- دفتر مطالعات و برنامه‌ریزی رسانه‌ها (۱۳۸۹)، «شبکه‌های اجتماعی»، گزارش راهبردی رسانه ۱۰، تهران.
- روحانی، مصطفی (۱۳۸۷)، «رسانه‌های گروهی و امنیت ملی»، تهران: نشر راهبرد.
- سایت اینترنتی امداد رایانه ایران (http://www.ircert.com).
- شاهپورنیا، حسین (۱۳۸۷) «فصلنامه هادی»، سال چهارم، شماره ۱۳، تهران.
- شکیب، علی‌حسن (۱۳۹۲)، «تهدیدات فضای سایبر بر امنیت ملی»، تهران: جلوه.
- صفری‌نژاد، احمد (۱۳۹۲)، «چگونگی بهره‌گیری از شبکه‌های اجتماعی»، تهران: دانشگاه امام حسین(ع).
- ضیایی‌پرور، حمید (۱۳۸۸)، «جنگ نرم سایبری در فضای شبکه‌های اجتماعی»، تهران: رسانه.
- ضیایی‌پرور، حمید (۱۳۸۸)، «ویژگی‌های شبکه‌های اجتماعی»، تهران: رسانه.
- کوک، ترور، هاپکینز (۱۳۸۷)، «آشنایی با قدرت web2»، تهران: ترجمه و نشر مؤسسه کارگذار روابط عمومی.
- کوهی، رضا (۱۳۹۲)، «داده‌کاوی شبکه‌های اجتماعی در فضای سایبری»، تهران: دانشگاه امام حسین(ع).
- یوسفی، کامبیز (۱۳۸۴)، «اصول و مفاهیم سیستم‌های مدیریت امنیت اطلاعات منطبق بر BS7799-2002»، تهران: گنج گوهر.