

بررسی نقش نبرد سایبری در آسیب‌شناسی فرهنگی و ارائه راهکارهای آن

عیسی خداپنده

چکیده

امروزه با کوچک‌تر و پیچیده‌تر شدن جهان به واسطه رشد روزافزون وسایل ارتباط جمعی از قبیل اینترنت و ماهواره معادلات گذشته در تنظیم روابط بین کشورها تا حدود زیادی به هم خورده و جای خود را به معادلات جدیدی داده است؛ به گونه‌ای که به جای به کارگیری مستقیم زور، توجه قدرت‌ها به استفاده از جنگ سایبری و ایجاد تغییرات از طریق مسالمت‌آمیز و شیوه‌های نوین مداخله در امور داخلی کشورها جلب شده است.

به هدایت عملیات نظامی بر اساس قوانین حاکم بر اطلاعات، جنگ سایبر گویند. هدف از این نوع جنگ، تخریب سیستم‌های اطلاعاتی و ارتباطاتی است. تلاش این جنگ در جهت شناسایی مسائلی است که دشمن به شدت از آن محافظت می‌کند؛ این جنگ حرکتی در جهت تغییردهی «توازن اطلاعات و دانش» به نفع یک طرف است؛ به خصوص اگر توازن نیروها برقرار نباشد. در واقع، به کمک دانش، سرمایه و نیروی کاری کمتری هزینه خواهد شد. این جنگ از فناوری‌های گوناگونی بهره می‌برد. از موارد برجسته این نوع فناوری‌ها می‌توان به فرماندهی و کنترل برای رسیدن به هوشمندی، توزیع و پردازش برای رسیدن به ارتباطات تاکتیکی، تثبیت موقعیت و شناخت هویت دوست و دشمن در زمینه مبادلات سیستم‌های جنگی هوشمند اشاره کرد. همچنین این نوع فناوری‌ها می‌توانند موجب اغفال، فریب و ایجاد اختلال در تجهیزات ارتباطاتی و اطلاعاتی دشمن شده و راهی برای نفوذ به آنها پیدا کنند. جنگ سایبر الزامات گسترده‌ای برای دکترین و سازمان‌های نظامی هم دارد. حرکت به سمت ساختار شبکه‌ای تا حدودی نیازمند فرماندهی و کنترل غیر متمرکز است، اما این همه مطلب نیست؛ فناوری جدید با تأمین نگاه بهتری از بالا، سبب بهبود مدیریت پیچیدگی‌ها می‌شود.

کلیدواژگان: فضای سایبری، اینترنت و فضای سایبر، آسیب‌های روانی، اعتیاد مجازی، تهدیدهای سایبری، نفوذگران سایبر

(۱) مقدمه

فضای سایبری چیست؟

فضای سایبر^۱ عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. به نظر می‌رسد به کارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفاً فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه‌های متنوعی از جمله خصلت‌های روان‌شناختی قابل توجه نیز دارد.

در منابع موجود آمده است که: واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر^۲ در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیسم‌ها در سیستم‌های انسانی، ماشینی (و رایانه‌ها) است. سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده و یا یک فضا که مربوط به دنیای رایانه و اطلاعات است.

در طی توسعه اینترنت، واژه‌های ترکیبی بسیاری از کلمه سایبر به وجود آمده است که به تعدادی از آنها اشاره می‌کنیم: فضای سایبر، شهروند سایبر^۳، پول سایبر^۴، فرهنگ سایبر^۵، راهنمایی فضای سایبر^۶، تجارت سایبر^۷، کانال سایبر^۸ و واژه "فضای سایبر" را نخستین بار ویلیام گیbson^۹ نویسنده داستان علمی‌تخیلی در

^۱-(Cyberspace)

^۲-(Norbert Wiener)

^۳-(Cybercitizen)

^۴-(Cybercash)

^۵-(Cyberculture)

^۶-(CyberCoach)

^۷-(Cyberbussiness)

^۸-(Cyberchannel)

^۹-(William Gibson)

کتاب نورومنسر^{۱۰} در سال ۱۹۸۴ به کار برده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق پیام‌نگار با یکدیگر ارتباط برقرار کنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابه‌جایی‌های فیزیکی نیست و تمامی اعمال فقط از طریق فشردن کلیدها یا حرکات موش‌واره (ماوس) صورت می‌گیرد. این عدم جابه‌جایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهت‌های فضای سایبر با حالت‌های ناهوشیاری، به ویژه حالت‌های ذهنی‌ای که در رویاها ظاهر می‌شوند، بپردازند. روند کاری یک کاربر رایانه در فضای سایبر دقیقاً نوعی یکی شدن یا محو شدن در درون واقعیتی متفاوت است؛ یعنی واقعیتی مجازی که ورای قوانین و واقعیت‌های واقعی است. به عبارت دیگر، مرز بین دنیای درون و بیرون تقریباً ناپدید می‌شود و دیگر گذر زمان معنایی ندارد. البته این سناریوی هر روز کاربران رایانه نیست؛ زیرا اغلب اوقات ما صرفاً به جهت انجام کاری مشخص و بدون آنکه به درون جهان مجازی فرو رویم به صفحه کلید ضربه می‌زنیم، اما اگر از استفاده‌های جزئی رایانه صرف نظر کنیم و از کاربران حرفه‌ایی و پروپاقرص آن پرس‌وجو کنیم درخواهیم یافت که بسیاری از آنها به راحتی لحظاتی را به یاد می‌آورند که گویی هیچ حائل و فاصله‌ای بین خود و رایانه‌شان احساس نمی‌کردند. در واقع می‌توان گفت که فضای سایبر گستره‌ایی از ذهن است که می‌تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. شما می‌توانید حالت‌های متنوع و متفاوت ذهنی را از قبیل تخیلات (خیال‌پردازی‌ها) خیال‌پروری‌ها، توهمات، حالات هیپنوتیستیک و سطوح گوناگونی از هوشیاری را در فضای مجازی تجربه کنید. تحت این چنین شرایط است که فضای سایبر همانند دنیای "رویا" می‌شود؛ دنیایی که وقتی ما به خواب فرو می‌رویم، پدیدار می‌شود. فضای سایبر را نمی‌توان تنها یک "بزرگ شاهراه اطلاعاتی" ساده دانست؛ زیرا تجربه ذهنی ما در فضای مجازی با تجربه ذهنی ما زمانی که بی‌هیچ هدف و ارزشی خیالبافی می‌کنیم، کاملاً متفاوت است. در واقع همانگونه که علم روان‌شناسی خواب شبانه را برای حفظ سلامتی، توسعه عاطفی و رشد شخصیت

یک فرد ضروری می‌داند، این فضای مجازی هم بیش از هر چیز دیگری در خدمت روان انسان است؛ زیرا مرزهای بین واقعیت‌های آگاهانه و ناآگاهانه را به هم نزدیک ساخته و می‌تواند درباره معنای "واقعیت" چیزهایی به ما بگوید. برای مثال محیط "پهلیس"^{۱۱} یک محیط چت گرافیکی است، کاربران در این محیط می‌توانند برای برقراری ارتباط با دیگران از بین صورتک‌های گرافیکی موجود در آن محیط، یک یا چند صورتک را برای بازنمایی شخص خود انتخاب کنند. این صورتک‌ها هر یک موقعیت یا حالت روانی خاصی را بیان می‌کند. بعضی از این حالت‌های "رویاگونه" در محیط "پهلیس" را می‌توان در دیگر فضاهای مجازی هم پیدا کرد. ولی تعدادی از این حالت‌ها تنها در محیط "پهلیس" وجود دارند و کاملاً بی‌نظیر و خاص هستند. مهم‌تر از همه این است که محیط "پهلیس" مانند رویا بسیار مجذوب‌کننده است؛ چرا که این محیط یک "تجربه بصری" جدی است.

۲) ابعاد آسیب‌های ناشی از اینترنت و فضای سایبر

از پدیده‌هایی که رایانه و پس از آن اینترنت همراه خود به ارمغان آورد، مخاطراتی بود که بر جای جای قلمرو گسترده‌اش، سایه انداخت. چنین مخاطراتی، چنانچه مورد بی‌توجهی جامعه و حکومت قرار گیرد، بسی بزرگ و گاه غیر قابل جبران خواهد بود؛ چراکه آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، موجب اختلال در رفتار شهروندان شده، جامعه را در رسیدن به فواید بی‌شمار این فناوری نوین ناکام می‌گذارد. این اختلالات، شهروندان را فرسوده و ناتوان کرده، فعالیت‌های روزمره آنان را مختل می‌کند. آسیب‌های اجتماعی و فرهنگی ناشی از آن، اعضای جامعه را در رفتار فردی با خانواده و رفتار اجتماعی با دیگر شهروندان و حکومت متزلزل و متأثر از فرهنگ‌های منحط بیگانه می‌نماید. هنجارها و ارزش‌های متعالی جامعه رو به زوال رفته، احساس امنیت و آرامش از جامعه رخت برمی‌بندد. ضمن اینکه آسیب‌های سیاسی آن، موجب تضعیف اقتدار و حاکمیت دولت شده، آن را در ایجاد وحدت ملی و امنیت اجتماعی و امنیت اطلاعاتی دچار چالش‌های جدی می‌کند.

در این مجال، به بررسی آسیب‌های فرهنگی و روانی فضای سایبر می‌پردازیم:

^{۱۱}-(Palace)

الف) آسیب‌های فرهنگی

۱) **کم‌رنگ شدن ارزش‌های مترقی:** هر جامعه صاحب ارزش‌هایی است که ناشی از فرهنگ آن است، اما برخی ارزش‌های مترقی در جوامع اسلامی است که به موجب تأثیر از فرهنگ بی‌بندوبار، و اباحه‌گر غرب در حال کم‌رنگ شدن است؛ ارزش‌هایی مثل حیا و عفت زن، اهمیت داشتن شخصیت انسان نه جنسیت آن و قبح عریان‌نمایی.

۲) **تضعیف فرهنگ‌های کم‌حضور:** از ویژگی‌های فضای سایبر این است که به شدت تحت تأثیر هر نوع عرضه گسترده‌ای قرار می‌گیرد. گرچه این فضا، گذرگاه فرهنگ‌های متنوع و گوناگونی است که هر یک در صدد عرضه خویش هستند، اما تنها فرهنگی پیشتاز خواهد بود که حضور پررنگ‌تر و گسترده‌تری داشته باشد. و بدین سبب است که در آن فرهنگ غالب، فرهنگی جز فرهنگ قدرتمند، اما منحط غرب نیست؛ چراکه با به کارگیری صحیح از امکانات وسیع و تلاشی وافر، به عرضه گسترده خود پرداخته و یک‌ه‌تاز این عرصه شده است.

به طور متوسط توسعه وب که یکی از مهم‌ترین ابزار عرضه فرهنگ است، هر سه ماه یک‌بار دو برابر می‌شود، اما این رشد روزافزون، به نفع فرهنگ غربی است؛ چراکه پررنگ‌ترین حضور از آن ایشان است. چنانکه حکومت زبان انگلیسی موجب شده است که کاربران با حضور در فضای سایبر، ضمن اینکه با زبان انگلیسی حاکم بر آن درگیر هستند، از زبان ملی خود دور شوند؛ به عنوان مثال، در چت‌های اینترنتی فارسی‌زبانان بیشتر از الفبای انگلیسی به جای الفبای فارسی استفاده می‌کنند که البته یکی از دلایل آن کمبود نرم‌افزارهای قدرتمند فارسی است. گسترش این کاربرد خود موجب تضعیف الفبا و زبان فارسی خواهد شد؛ به ویژه با توجه به اینکه علم و فناوری که از ضروریات زندگی است، در این فضا به صورت زبان انگلیسی نمود یافته است. تمامی نشریات، متون و منابع دست اول - حتی در کشورهای غیر انگلیسی - به این زبان می‌باشد. از این رو، دانستن زبان انگلیسی از لوازم حضور فعال در فضای سایبر شده است. آموزش، پژوهش و ارتباطات نمی‌تواند به حرکت پیش‌رونده خود ادامه داده و نیازهای جامعه را پاسخ دهد، مگر اینکه زبان انگلیسی را به کار گیرد و این خود به صورت طبیعی موجب سیطره فرهنگ غرب بر عرصه‌های گوناگون جوامع به ویژه جوامع اسلامی می‌شود. بدین وسیله، ارزش‌ها، روش‌ها و هویت‌های مطلوب فرهنگ غربی بر جوامع تزریق

شده، فرآیند دگرگونی عناصر فرهنگی سرعت خواهد گرفت. آری، در شرایطی که دشمنان فرهنگ و غارتگران اندیشه‌های راستین اسلامی با درک قابلیت بالای این شاهراه ارتباطی و اطلاعاتی، از آن در اشاعه خواسته‌های نفسانی و آرمان‌های دنیایی خود کمال استفاده را می‌کنند، هرگز نباید لحظه‌ای از استفاده مطلوب از این ابزار پر قدرت فرهنگ‌ساز غافل شد.

۳) تضعیف اعتقادات و گسترش شبهات فکری: گرچه دستیابی آسان به انواع اطلاعات از مزایای فضای سایبری است، اما معایبی نیز دارد. از جمله اینکه طرح و نشر انواع شبهه در آن، موجب تزلزل در باورهای کاربران سست عقیده و کم‌اطلاع می‌شود. فضای سایبر چاقویی دولبه است که ما می‌توانیم از آن به سود خود مدد بگیریم، اما هجمه و تنوع و گسترش فرهنگ مهاجم غربی، به حدی است که در شرایط فعلی کوشش‌های مدافعان فرهنگی مسلمان را بسیار کم‌اثر می‌کند؛ خاصه اینکه مدیریت اصلی اطلاعات نیز در دست غرب و غریبان است. البته بهترین راه حل تنها انفعالی عمل کردن و اکتفا کردن به پاسخگویی به شبهات نیست، بلکه این پاسخگویی باید همراه با تهاجم نیز باشد؛ به این معنا که باورهای فرهنگ مهاجم را نیز با سؤالاتی که در مورد باورها و نگرش‌هایشان وجود دارد، هدف قرار دهیم و هیمنه ظاهری آنان بشکنیم.

۴) رواج سطحی‌نگری فکری: آزادی بیان و طرح اندیشه‌های متضاد در فضای سایبر، از اهداف اولیه ایجاد چنین فضایی است، اما چنانچه اندیشه‌ای بدون هیچ بنیان و اساس معتبری در این فضا مطرح شود، ثمره آن انباشته شدن اندیشه‌های بسیاری است که توان بررسی و نقد و تحلیل همه آنها از عهده مخاطبان خارج است. و بدین سبب، کاربران بدون بررسی و تحقیق در مبانی و زوایای پنهان اندیشه‌های نوظهور، به سبب کثرت و رواج بی‌حد و حصر آن در فضای سایبر، از آن متأثر می‌شوند. در نتیجه، روحیه حق‌پذیری کاربران به ویژه جوانان، به سطحی‌نگری و مسامحه‌کاری در پذیرش اندیشه‌های نوظهور مبدل خواهد شد.

۵) ایجاد سردرگمی: آنگاه که کودکی را بخواهند آموزش دهند، ابتدا او را با مفاهیم ساده‌ای در حد فهم او آشنا می‌کنند. طرح مفاهیم متنوع و اندیشه‌های متضاد برای او، ثمره‌ای جز حیرت نخواهد داشت. فضای سایبر گرچه مولد آزادی بیان و تضارب آرا است، اما انباشت اطلاعات خوب و بد، گزینش اطلاعات صحیح را

دشوار کرده و طرح نامحدود و طبقه‌بندی نشده آن، موجب سردرگمی کسانی خواهد شد که در تحلیل افکار و اندیشه‌ها دچار ضعف هستند. از این رو، ضروری است که پیش از هر چیز کاربری صحیح و طبقه‌بندی‌شده این فضا را به کاربران بیاموزیم.

۶) گسترش اباحه‌گری عملی: حفظ حرمت قوانین اجتماعی و رعایت آموزه‌های اخلاقی، از ریشه‌ای‌ترین اصول هر فرهنگی است. بدیهی است با گسترش اباحه‌گری در فضای سایبر، در نهایت این روند در میزان ارتکاب اعمال غیر اخلاقی و ناهنجار در فضای جامعه نیز تأثیر خواهد گذاشت. منشأ برخی از اعمال خلاف اخلاق در سطح جامعه، مباح شدن آن در فضای سایبر است.

۷) به خطر افتادن حقوق مادی و معنوی مؤلفان: یکی از نگرانی‌های مؤلفان آثار علمی، ادبی و یا هنری ارائه آثارشان به صورت دیجیتال است. با توجه به گسترش روزافزون سرقت داده‌های گوناگون و نرم‌افزارها و نیز عدم توانایی مسئولان در برخورد با این قبیل جرایم و دشوار بودن نظارت و حفاظت از داده‌ها، حقوق مادی و معنوی مؤلفان در فضای سایبر دو چندان به خطر خواهد افتاد؛ چراکه با توجه به قدرتمند شدن ابزارهای قفل‌شکن و نبود نظارت لازم بر فضای سایبر، مؤلفانی که بخواهند از منافع مادی و معنوی اثر خویش بهره ببرند، از ارائه اثرشان در غالب داده‌های الکترونیکی خودداری می‌ورزند.

۸) گسترش محصولات فرهنگی: فرهنگ‌های منحن به ویژه فرهنگ غربی به صورت محصولات فرهنگی اعم از فیلم، عکس، متن، بازی‌های رایانه و اینترنتی از سوی غرب و گاه شرق، تولید و در فضای سایبر تبلیغ و توزیع می‌شوند. بدین سان یکی از خطرهای ناشی از فضای سایبر متوجه کشورهایی است که دارای فرهنگ‌های متضاد با فرهنگ حاکم بر فضای سایبر است. به ویژه کاربران مسلمان، که عمدتاً با وجود برخورداری از فرهنگی غنی، از استفاده از محصولات قوی فرهنگی متناسب با فرهنگ خود محروم‌اند.

ب) آسیب‌های روانی

۱) افسردگی و انزوا: کاربران، بیشتر ترجیح می‌دهند در محیطی آرام و خلوت، از اینترنت استفاده کنند تا هم بهتر بتوانند از اطلاعات آن بهره ببرند و هم با تمرکز و سرعت بیشتر، از اتصال‌های طولانی مدت جلوگیری کرده، هزینه‌های حاصل از آن

را کاهش دهند. اما این نوع خلوت و انزوا در طولانی مدت، برخی مشکلات روانی مانند گوشه‌گیری و در نهایت افسردگی را در پی دارد.

(۲) گمنامی و نامرئی بودن: گمنامی و نامرئی بودن کاربران، از دیگر ویژگی‌های روابط اینترنتی است که موجب پیدایش آسیب‌های جدی اخلاقی و روانی در افراد می‌شود. در فضای سایبر می‌تواند هر نقابی را بر خود بپوشاند و بدین وسیله هر چه می‌خواهد، می‌گوید و هر کاری که بخواهد، انجام می‌دهد؛ بدون اینکه ترس از شناخته شدن و رسوا شدن داشته باشد. این ویژگی موجب کاهش خویشتن‌داری و بازدارندگی کاربران در برابر اعمال ناهنجار اخلاقی و ضد اجتماعی خواهد شد. هدف از اجرای بسیاری از مجازات‌ها در سطح جوامع، ایجاد حس بازدارندگی در میان افراد جامعه به ویژه مجرمان و افراد دارای حالت خطرناک است.

(۳) بحران هویت و اخلال در شکل‌گیری شخصیت: عناصر سه‌گانه هویت، یعنی: شخص، فرهنگ و جامعه، هر یک در تکوین شخصیت فرد نقش مهمی را ایفا می‌کنند. هویت شخصی، ویژگی بی‌همتای فرد را تشکیل می‌دهد. هویت اجتماعی در پیوند با گروه‌ها و اجتماعات مختلف قرار گرفته و شکل‌گیری آن، متأثر از ایشان است. در نهایت، هویت فرهنگی، برگرفته از باورهای است که در عمق وجود فرد به واسطه تعامل او با محیط پیرامون و آموزه‌های آن، از بدو تولد تا کهنسالی جای گرفته است.

از آنجا که فضای سایبری، صحنه‌ای فرهنگی و اجتماعی است که فرد خود را در موقعیت‌های متنوع، نقش‌ها و سبک‌های زندگی قرار می‌دهد، خود زمینه‌ای است برای آسیب‌پذیری شخصیت کاربر که در نتیجه، موجب چند شخصیتی شدن کاربر خواهد شد. در فضای سایبر بیش از آنکه هویت ظاهری فرد مطرح شود، درون‌مایه‌های افراد بروز می‌کند. هر کس در صدد بیان اندیشه‌ها و علاقه‌مندی‌های خویش است. از سوی دیگر، گاهی برخی از ویژگی‌های شخصیتی مانند: سن، تحصیلات، محل سکونت و حتی جنسیت در اینترنت از بین می‌رود؛ به عنوان نمونه، بسیاری از افرادی که در اتاق‌های چت مشغول گفتگو با یکدیگر هستند، با مشخصاتی غیر واقعی ظاهر شده و از زبان شخصیتی دروغین که از خود ساخته‌اند

و آن را به مخاطب یا مخاطبان خود معرفی کرده‌اند، صحبت می‌کنند و با این حال، همین شخصیت‌های ناشناس چه تأثیرات مختلفی بر یکدیگر دارند.

۴) اعتیاد مجازی^{۱۲}: اعتیاد مجازی، استفاده بیش از حد از اینترنت است تا آنجا که بدون استفاده از آن فرد احساس کمبود می‌کند و روابط او با محیط متأثر از استفاده مکرر و دیوانه‌وار فرد شده، از حالت عادی خارج می‌شود. نبود روابط پایدار و صمیمی با دیگران، نداشتن اعتماد به نفس و به طور کلی شکست در عرصه‌های گوناگون زندگی، زمینه را برای اعتیاد افراد به اینترنت فراهم می‌کند. نتایج پژوهش یانگ (۱۹۹۷) در این زمینه نشان داد که یکی از دلایل مهم اعتیاد به اینترنت در افرادی که روابط عمومی کمتری دارند، به دست آوردن حمایت‌های اجتماعی است؛ زیرا حمایت‌های اجتماعی با اعمالی چون ورود به اتاق گپ‌زنی در میان اعضا در فضای سایبر زودتر به وجود می‌آید. از دیگر پیامدهای اعتیاد اینترنتی، مشکلات خانوادگی و تأثیر آن بر روابط زناشویی، والدین و فرزندان است. امروزه اصطلاح «بیوه اینترنتی» برای همسر معتاد به اینترنت اطلاق می‌شود. آمار نشان می‌دهد که اعتیاد به اینترنت ممکن است به فروپاشی خانواده و طلاق منجر شود. شاید باور کردن اینکه شخصی همسر خود را فقط به علت ارتباط با فرد دیگر در اینترنت ترک می‌کند، برای کسانی که به اینترنت اعتیاد پیدا نکرده‌اند، وحشتناک به نظر برسد، ولی این مسأله هر روز در دنیای اینترنت اتفاق می‌افتد. در مواردی اعتیاد به اینترنت موجب از دست دادن شغل نیز شده است. منشأ اغلب اعتیادهای مجازی را می‌توان عدم کنترل و کاربرد صحیح از اینترنت دانست؛ چراکه کاربرد اینترنت در جهت هرزه‌نگاری بازی‌های رایانه‌ای و گپ‌زنی به واسطه جذابیت‌هایی که دارد، به مرور در فرد وابستگی و اعتیاد ایجاد کرده، منجر به اعتیاد مجازی می‌شود. از این رو، برخورد با هرزه‌نگاری و آموزش صحیح استفاده از اینترنت در جلوگیری از این اختلال در سطح جامعه کارساز است.

۵) انحرافات اخلاقی: از جمله آثار مخرب فضای سایبر، به وجود آمدن انحرافات جنسی و اختلالات جنسی است. اینترنت به دلیل رویکرد آزاداندیشی در روابط جنسی از سوی گردانندگان اصلی آن (غرب و به ویژه آمریکا) و نگرش تجاری

^{۱۲}-(VIRTUAL ADDICTION)

نسبت به مسائل جنسی، موجب پدید آمدن پدیده شومی به نام هرزه‌نگاری^{۱۳} و هنر پلید شهوانی^{۱۴} و رواج سرسام‌آور آن شده است. این پدیده مرزهای اخلاقی را در هم می‌شکند و تهدیدی برای فرهنگ‌ها به خصوص فرهنگ‌های دینی همچون فرهنگ اسلامی است. اصولاً، پورنوگرافی (هرزه‌نگاری) به عنوان نمایش تصویری و یا کلامی رفتارهای جنسی است که با هدف ارضای خواسته‌های جنسی دیگران تعریف می‌شود. اینگونه مطالب و تصاویر که در پی تحریک جنسی دیگران عرضه می‌شود، معمولاً به ارضای غیر طبیعی جنسی مراجعه‌کنندگان آن می‌انجامد. نکته دیگر اینکه رجوع به اینترنت برای دسترسی به مطالب مستهجن، صرفاً به افراد نابهنجار خلاصه نمی‌شود و حجم قابل توجهی از مراجعان را افراد طبیعی تشکیل می‌دهد.

۳) تهدیدهای سایر

تهدیدهای سایر بسیار زیاد و متنوع هستند. یک حمله تروریستی می‌تواند به شکل الکترونیکی، فرکانس رادیویی و حملات مبتنی بر رایانه، به اجزای ارتباطی یا اطلاعاتی کنترل‌کننده زیرساخت‌های حیاتی باشد. این تهدید عبارتند از:

(الف) ویروس‌های رایانه‌ای: ویروس‌ها یا «برنامه‌های خود همانندسازی»، با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند.

(ب) عنکبوت‌های موتورهای جستجو: بحران‌سازهای رایانه‌ای هستند که با داشتن پالس‌های الکترومغناطیسی، می‌توانند دیسک سخت یک رایانه را ذوب کنند.

(ج) اسب‌های تروا: به ظاهر برنامه‌هایی سودمند یا مفیدند، اما پس از مدتی کدهایی خطرناک آزاد می‌کنند.

(د) نوعی ویروس با عنوان خرگوش: خرگوش‌ها به رایانه دستور می‌دهند، تا وظایف بی‌فایده را به صورت بی‌پایان انجام دهند؛ به این ترتیب، همه توان رایانه به این کارها اختصاص می‌یابد و دستگاه در عمل از مدار خارجی می‌شود.

(هـ) کرم‌ها: در یک رایانه جاگیر می‌شوند و به صورت مرتب فضای رایانه را اشغال می‌کنند.

^{۱۳}-(Pornography)

^{۱۴}-(Erotice art)

(و) بمب‌های منطقی: آنها تعمداً زیانبار ساخته می‌شوند، اما مانند ویروس‌ها تکثیر نمی‌شوند و معمولاً یک دوره زمانی در رایانه غیر فعال باقی می‌مانند و با سر رسیدن تاریخ مشخص‌شده، منفجر می‌شوند. در این هنگام، ممکن است ویروس یا کرمی خطرناک را آزاد کنند.

۴) ویژگی‌های فضای سایبر

الف) جهانی و فرامرزی بودن: از ویژگی‌های منحصربه‌فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد.

مرزهای جغرافیایی تاکنون نتوانسته است از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار می‌نماید.

ب) دستیابی آسان به آخرین اطلاعات: چنانچه بخواهید به آخرین مقاله، کتاب و یا خبری که در زمینه تخصصی، در سطح جهان منتشر شده، دست یابید، ساده‌ترین و سریع‌ترین راه، استفاده از فضای سایبر است.

ج) جذابیت و تنوع رسانه‌ها: از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است؛ به ویژه آنگاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی‌های منحصربه‌فردی که در تنوع و جذابیت فضای سایبر تأثیر به‌سزایی دارد، مشتری‌محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می‌تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان‌تر و روزآمدتر است و این توانایی را به داده‌پردازان، فروشندگان و عرضه‌کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته‌های مشتریان و مخاطبان خود مطلع شوند.

د) آزادی اطلاعات و ارتباطات: معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این رو، شما هر نوع اطلاعاتی را که بخواهید - اعم از فرهنگی، سیاسی و اقتصادی - بدون محدودیت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.

۵) سلاح‌های سایبر

سلاح‌های سایبر شامل موارد زیر می‌شود:

الف) ابزارهای آفندی:

ویروس‌های رایانه‌ای، اسب‌های تروا، ابزارهای عدم دسترسی به سرویس

ب) ابزارهای دارای کاربری دو منظوره:

اسکنرهای آسیب‌پذیری پورت و ابزارهای پایش شبکه

ج) ابزارهای پدافندی:

رمزنگاری و دیواره آتش

۶) انواع نفوذگران در جنگ سایبر

الف) گروه نفوذگران کلاه سفید^{۱۵}: هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. هکرها کلاه سفید متخصصان شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا می‌کنند و به مسئولان گزارش می‌دهند.

ب) گروه نفوذگران کلاه سیاه^{۱۶}: اشخاصی هستند که وارد رایانه قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن ویروس و غیره می‌پردازند.

ج) گروه نفوذگران کلاه خاکستری^{۱۷}: اشخاصی هستند که حد وسط دو تعریف بالا قرار می‌گیرند.

د) گروه نفوذگران کلاه صورتی^{۱۸}: این افراد آدم‌های کم‌سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

۷) انواع حملات نفوذگران

الف) شنود^{۱۹}: در این روش نفوذگر می‌تواند به شکل مخفیانه از اطلاعات نسخه‌برداری کند.

^{۱۵}-(White hat hackers)

^{۱۶}-(Black hat hackers)

^{۱۷}-(Gray hat hackers)

^{۱۸}-(Pink hat hackers)

^{۱۹}-(interception)

(ب) **تغییر اطلاعات^{۲۰}**: در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد.

(ج) **افزودن اطلاعات^{۲۱}**: در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

(د) **وقفه^{۲۲}**: در این روش نوع نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

۸) نقاط ضعف اصلی در دفاع سایبر

(الف) بررسی هویت و مکان مهاجم؛

(ب) شناسایی نیت مهاجم؛

(ج) تشخیص حمله‌های از قبل طراحی شده؛

(د) بررسی و ارزیابی تلفات بعد از جنگ.

۹) نمونه‌ای از حملات سایبری

در ادامه، پنج نمونه خبرساز از حملات سایبری را که در فضای مجازی رخ داده‌اند و برخی راهکارهای مقابله با آنها را مشاهده می‌کنید:

۱) کرم استاکس نت ۲۰۱۰

متخصصان این کرم را به عنوان یکی از پیچیده‌ترین کرم‌های رایانه‌ای که تا به حال مشاهده شده می‌شناسند. این کرم به سیستم‌های رایانه‌ای صنعتی که سیستم‌های ماشینی نیروگاه‌ها و کارخانه‌ها را تحت کنترل دارند، حمله می‌کند. این کرم با بهره‌برداری از چهار نقطه ضعف که پیش از این در سیستم عامل ویندوز ناشناخته باقی مانده بودند، فعالیت می‌کند. برای مثال یکی از آسیب‌پذیری‌های ویندوز به استاکس نت کمک می‌کند در میان شبکه‌های محلی گسترش پیدا کند، دیگری به پخش شدن کرم در میان سخت‌افزارهای قابل جابه‌جایی از قبیل حافظه‌های USB و یا درایورهای CD کمک می‌کند. به گفته متخصصان قابلیت‌های این کرم در استفاده از بیش از یک نقطه ضعف سیستم عامل رایانه‌ها کاملاً بی‌سابقه است و نشان از حمایت دولتی و پشتیبانی مالی شدید از این کرم رایانه‌ای دارد.

^{۲۰}-(modification)

^{۲۱}-(fabrication)

^{۲۲}-(interruption)

با وجود اینکه هنوز تعیین قطعی هدف اصلی استاکس نت امکان‌پذیر نیست، اما حملات این کرم به شکلی مشخص و نامتناسب به سوی ایران متمرکز بوده است. هر چند که این عملیات ناموفق بود.

۲) عملیات آنورا ۲۰۰۹

گوگل، آدوبی و حدود ۳۰ شرکت دیگر اعلام کردند قربانی حملات به شدت پیچیده سایبری شده‌اند. هکرها طی این حملات توانسته بودند با بهره‌برداری از نقطه ضعفی شناخته‌نشده در مرورگر اینترنت اکسپلورر، به اطلاعات حیاتی و خصوصی این شرکت‌ها دست پیدا کنند.

نکته کلیدی اینکه نیاز به افزایش احتیاط در میان کارمندان شرکت‌های چندملیتی است تا در هنگام استفاده از رایانه‌های شرکت دقت کافی را به خرج دهند؛ زیرا در شرکت گوگل یک کلیک کوچک و ناآگاهانه بر روی یک پیغام کوتاه منجر به بروز تمامی این مشکلات شد.

۳) فرماندهی مرکزی ایالات متحده آمریکا ۲۰۰۸

برخی از سازمان‌ها به ویژه سازمان‌های دولتی، رایانه‌های خود را از دسترس عموم و یا عضویت در شبکه‌های غیر ایمن خارج می‌کنند تا از بروز شکاف‌های امنیتی در آن جلوگیری کنند.

در زبان رایانه‌ای این شکاف به شکاف هوایی شهرت دارد. با این همه با ظهور رسانه‌های قابل حملی مانند حافظه‌های USB و CDها تبهکاران سایبری فرصتی مناسب را برای نفوذ به درون شبکه‌های بسیار ایمن به دست آوردند.

در سال ۲۰۰۸ وزارت دفاع آمریکا با چنین حملاتی مواجه شد که منبع اصلی آن یک حافظه USB غیر ایمن بود که به یک لپ‌تاپ وصل شده بود. این حافظه حاوی کدهای مخربی بود که در سرتاسر رایانه‌های وزارت دفاع آمریکا پخش شد و اطلاعات موجود در این رایانه‌ها را به سرورهای خارجی ارسال کرد.

۴) گرجستان ۲۰۰۸

در سال ۲۰۰۸ و درست یک هفته پس از یورش روسیه به گرجستان، حمله‌ای سایبری، دولت و وبسایت‌های رسانه‌ای این کشور را دچار اختلال کرد. همانطور که در سال ۲۰۰۷ نیز جو سیاسی اقتضا می‌کرد کرملین دستور یک حمله سایبری را

به استونی صادر کند. با این تفاوت که افرادی که به گرجستان حمله کردند سیستم‌های رایانه‌ای سازمانی این کشور را نیز بی‌نصیب نگذاشتند.

این حمله به "باتنت" شهرت داشته و به گونه‌ای است که هر شهروند روسی می‌توانسته است آگاهانه یا ناآگاهانه و با دانلود نرم‌افزاری سبک به ایجاد اضافه بار بر وب‌سایت‌های دولتی و سازمانی گرجستان کمک کرده باشد.

(۵) استونی ۲۰۰۷

در این سال کشور استونی در معرض سیلی از حملات سایبری قرار گرفت که کل زیرساخت‌های اینترنتی کشور را تحت تأثیر خود قرار دادند و البته هدف اصلی وب‌سایت‌های دولتی و سازمانی، بانک‌ها و روزنامه‌ها بودند.

با توجه به زمانبندی حملات که در زمان مجادله این کشور و روسیه بر سر برداشتن یادبود شوروی از پایتخت استونی بود، مقامات استونی روس‌ها را عامل اصلی این حملات می‌دانند. با این حال مثل همیشه امکان ردیابی منشأ اصلی این نوع از حملات وجود نداشته و نخواهد داشت.

(۱۰) راهکارها

(۱) ایجاد نهادهای ویژه حقوقی برای مطالعات حقوقی سایبر، به ویژه تأسیس رشته‌های دانشگاهی و تربیت قضات و بازپرس‌هایی که در زمینه جرایم سایبر تخصص داشته باشند.

(۲) ایجاد قوانین جدید و سازگار به محیط سایبر؛ زیرا قوانین سنتی جوابگوی مشکلات نیست.

(۳) قانونگذاری در این زمینه نیازمند شناخت مختصات فضای جدید و تفاوت‌های ماهوی آن با فضای سنتی است.

(۴) شکل‌گیری مفاهیم جدید به منظور قانونگذاری در این فضا؛ مانند صحنه جرم سایبر، ادله الکترونیکی، صلاحیت مجازی و مواردی از این قبیل.

(۵) توجه به مقتضیات خاص جامعه ایرانی و ملاحظات مذهبی در تدوین متون قانونی سایبر و تسریع تشکیل روند دادسرای ویژه جرایم رایانه‌ای در کشور.

(۶) راه‌اندازی هرچه سریع‌تر دیتاسترهای داخلی به منظور کاهش آسیب‌پذیری در برابر اقدامات خرابکارانه یا مسدودسازی سایت‌ها.

کتابنامه

- ۱) <http://www.hamshahrionline.ir>
- ۲) <http://vageiat.parsiblog.com>
- ۳) <http://www.newit.blogsky.com>
- ۴) <http://www.rasekhoon.net>
- ۵) <http://www.scict.ir>
- ۶) <http://mattlab.mihanblog.com>
- ۷) <http://www.itexperts.ir>
- ۸) <http://www.gerdab.ir>