

بررسی تهدیدات فناوری اطلاعات و نقش امنیتی پلیس در فضای سایبر

بهزاد پورنقدی^۱

چکیده

توسعه علوم رایانه و فناوری اطلاعات و ارتباطات تمامی علوم موجود در جهان را تحت تاثیر خود قرار داده است و هر جامعه ای برای جلوگیری از عقب ماندگی علمی و تکنولوژیک به ناچار باید با پیشرفت علوم و فناوری همگام و همراه شود. با توجه به آماج حملات فرهنگی و تهدیدات فناوری اطلاعات و شبکه اینترنت در زمینه های مختلف اجتماعی، فرهنگی، اخلاقی، سیاسی، انتظامی و تعداد بسیار زیاد کاربران ایرانی در اینترنت، برای تاثیرگذاری بیشتر و کاهش هزینه های فیلترینگ و کنترل دسترسی برای مقابله با تهدیدات سایبری و آینده های اجتماعی آن، پیشنهاد می گردد نیروی انتظامی با هدایت منابع و امکانات موجود در جهت افزایش سطح آگاهی و بلوغ فکری کاربران و فرهنگ سازی، پایه های امنیت اجتماعی سایبری را مستحکم نماید. شتاب توسعه علوم بشری و پیشرفت فناوری های نوین، دستاوردهای جدید علمی را برای انسان به ارمغان آورده است. لیکن ورود به عرصه های جدید علمی و فناوری همواره پیامدهایی را برای امنیت اجتماعی و مسائل اخلاقی به همراه خواهد داشت. همچنین غفلت مسئولین در آموزش و توجه به کاربری فناوری های نوین باعث انحراف و اغفال کودکان، فرزندان و نوجوانان خواهد شد. برای استفاده هر چه امن تر و مطمئن تر از فناوری اطلاعات، پرداختن به دو مقوله آموزش اجتماعی و ایجاد و توسعه پلیس الکترونیک و تجهیز پلیس مجازی به ابزار های سخت افزاری و نرم افزاری مورد نیاز آن می باشد.

واژگان کلیدی: آینده های سایبر، امنیت اجتماعی، فیلترینگ، کنترل دسترسی

^۱ دانشجوی دکترای فناوری اطلاعات، عضو باشگاه پژوهشگران جوان - دانشگاه آزاد اسلامی، واحد تهران مرکزی
behzad_pournaghdhi@yahoo.com

مقدمه

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و در عین حال نظام مند، معقول و هدفمند به منظور مصون سازی این بستر از تهدیدات موجود در جهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای سایبر و مخاصمات امروز این فناوری نوین را می طلبد. با امکانات و گزینه‌های فراوانی که رسانه‌های جدید در عصر اطلاعات در اختیار افراد جامعه قرار می دهند، کاربران دائماً با محرک های جدید و انواع مختلف رفتارهای اجتماعی و اخلاقی آشنا می‌شوند. این فضا هویت نامشخص و پیوسته متحولی را می‌آفریند و بیشترین تأثیر آن برای نسلی است که در مقایسه با نسل قبل با محرک های فراوانی مواجه است. همچنین از طریق رسانه‌های نوین و فناوری اطلاعات در فضای سایبر^۱، افراد جامعه خط مفروض میان فضای عمومی و خصوصی را تجدید سازمان می کنند و این امکانی است که جامعه فعالانه از آن استفاده می‌کند. شتاب توسعه علوم بشری و پیشرفت فناوری های نوین، دستاوردهای جدید علمی را برای انسان به ارمغان آورده است. لیکن ورود به عرصه های جدید علمی و فناوری همواره پیامدهایی را برای امنیت اجتماعی و مسائل اخلاقی به همراه خواهد داشت. پیشرفت و توسعه علمی با یک فرآیند دو جانبه همراه بوده است، یکی جنبه خدمات و ارزش های ارایه شده توسط فناوری جدید و دیگری فرهنگ کاربردی امنیتی و اخلاقی علوم نوظهور می باشد. خدمات و دستاوردهای فناوری های نوین در ارتقاء سطح کیفی زندگی انسان ها نقش مهمی ایفا می کند و به رفع نیازها، مشکلات، خواسته ها و علایق بشری می پردازد. در مقابل ارایه خدمات و راهکارهای فنی، مسائلی همچون: امنیت، اخلاق علمی،

^۱ Cyber

فرهنگ کاربری و اخلاقی مورد توجه و بحث و بررسی می باشد. مسائل امنیتی و اخلاقی سایبری از دو جنبه مورد بررسی قرار می گیرد:

۱- رعایت اخلاق علمی و موارد امنیتی در تولید فناوری مبتنی بر سایبر (توسط عرضه کنندگان فناوری).

۲- مسائل اخلاقی و امنیتی کاربری فناوری اطلاعات (توسط کاربران و مصرف کنندگان سایبری).

موضوعی که باعث اهمیت امنیت اجتماعی سایبر در دهه اخیر شده است، رشد پرشتاب علم و فناوری همزمان با ضعف نظام های سنتی اخلاقی و امنیتی در جوامع بود. در نتیجه این پرسش به میان آمد که با این مقیاس از تصرف ذهنی و علمی در عالم توسط انسان که با پیشرفت دانش و فناوری ظاهر می شود، آیا توسعه فناوری اطلاعات و فضای سایبر متعهد به کیفیتی مبتنی بر منطق امنیت اجتماعی و مصلحت جمعی نیز هست؟

بیان مساله

امنیت در فضای سایبری و سلامت دیجیتالی یک زمینه نوظهور از برخورد انفورماتیک، بهداشت روانی و ارتباطات در عصر اطلاعات است که از طریق شبکه جهانی اینترنت، فضای سایبر و فناوری های مرتبط با آن ارتقا و تکامل می یابد. امنیت سایبری را نه تنها به عنوان یک توسعه فنی بلکه به عنوان حالتی روحی، طرز تفکر و یک حرکت عمومی جهانی می توان توصیف کرد. میزان استفاده جمعی و عمومی از فناوری اطلاعات و ابزار اینترنت هر روز بیشتر و فراگیرتر می شود. به طوری که در کشور ایران تنها ظرف مدت چند سال یعنی از سال ۱۳۸۰ تا ۱۳۸۷ تعداد کاربران

اینترنت از ۲ به ۱۸ میلیون نفر رسیده است.^۱ این میزان گسترش فناوری اطلاعات با پیامدهای اخلاقی و امنیتی نیز همراه خواهد بود که در ادامه به برخی از آنها اشاره می شود. فناوری اطلاعات و ابزار گسترده اینترنت توانایی و امکان انتقال متن، ایمیل، تبادل اطلاعات و دسترسی به پایگاه های داده ای و اطلاعاتی، دسترسی به تصاویر، پخش فیلم و موسیقی، چت و گفتگوی مجازی، شرکت در بحث های گروهی و امکانات دیگری را دارد که با عدم رعایت مسائل امنیتی در کاربری این امکانات و دسترسی های غیر مجاز به اطلاعات و داده ها، پدیده های غیر اخلاقی متعددی را به وجود می آورد که برخی از آنها عبارتند از: هک و نفوذ به رایانه های شخصی و اداری، اقدام علیه امنیت ملی، نشر اکاذیب و فعالیت های انحرافی سیاسی و اجتماعی، ترویج عقاید باطل و فرقه های انحرافی مذهبی از قبیل شیطان پرستی و متال و ...، سرقت و دزدی اطلاعات و داده ها، دسترسی غیر قانونی به منابع اطلاعاتی و مالی، انتشار افکار و رفتارهای غیر اخلاقی و مخالف با هنجارهای جوامع بشری، سوء استفاده های جنسی، سوء استفاده های مالی و اطلاعاتی، دزدی هویت و ترویج فساد. فناوری اطلاعات و اینترنت تفکرات و رویاهای افراد را تحریک می نماید، زیرا این فناوری امکان انتشار جهانی ایده ها و نظریات آنها را فراهم می سازد. دستیابی به تصاویر مبتذل جنسی و خشونت بار یکی از پدیده های ضد اخلاقی است که مخاطبان و کاربران فناوری اطلاعات به ویژه کودکان و نوجوانان را در معرض تهدید و کنش های نامناسب اخلاقی قرار می دهد. ارتباطات و روابط کاربران در محیط های مجازی و فریب های هویتی ناشی از آن یکی دیگر از پیامدهای اخلاقی در عصر اطلاعات است و همین موضوع باعث بی اعتبار شدن هویتی در رسانه های ارتباطی و فناوری اطلاعات شده است. از یک سو متخصصان و پدید آورندگان علوم و فناوری اطلاعات ملزم به رعایت نکات اخلاقی و حقوق کاربری خاص خود

۱- گزارش اظهارنظر کارشناسی درباره لایحه جرائم رایانه ای؛ مرکز پژوهش های مجلس شورای اسلامی، ۱۳۸۷/۵/۱۹

هستند. انتشار کدهای مخرب و جاسوسی اطلاعات یکی از عوامل مخرب و ضد اخلاقی در این زمینه است.

امنیت سایبری و هویت مجازی

از مسائل مهم امنیت اجتماعی که در دنیای فناوری اطلاعات مطرح است، هویت مجازی^۱ کاربران و امنیت سایبری آنان در دنیای مجازی اینترنت است. پدیده ای به نام هویت مجازی این امکان را به کاربران فناوری اطلاعات می دهد که تحت هر عنوانی به معرفی خود بپردازند و از مخاطبان خود سوء استفاده نموده و از این راه به اهداف و مقاصد غیر اخلاقی خود برسند. این موضوع به قدری دارای اهمیت است که گاهی منجر به تباهی زندگی افراد جامعه می شود. پایبندی به هنجارهای خانواده و اصول مذهبی و دینی در کنار آموزش صحیح کاربری و استفاده از فناوری اطلاعات، به ویژه برای کودکان، نوجوانان و جوانان راه حلی مناسب برای جلوگیری از ناهنجاری های ضد اخلاقی تکنولوژیکی است. از دیگر موارد ضد اخلاقی و نفوذ به حریم خصوصی دیگران، دزدی اطلاعات شخصی مانند: رمزهای عبور^۲، حساب بانکی، دسترسی غیر قانونی به اطلاعات دیگران، نفوذ به کامپیوترهای شخصی^۳ و انجام فعالیت های مخرب، خرابکاری و ایجاد بحران در سیستم های کامپیوتری ادارات و سازمان ها، افشای اطلاعات شخصی افراد حقیقی و حقوقی، ارسال اطلاعات دروغ و نامه های تحریف شده، شیوع و انتشار ویروس و برنامه های جاسوسی^۴ و مسائلی از این قبیل می باشد.

^۱ Virtual Personality

^۲ Password

^۳ Hack

^۴ Spy Programs

تهدیدات اخلاقی و اجتماعی در فضای سایبر

از آنجا که فناوری اطلاعات تحولات سیاسی و اجتماعی وسیع و شگرفی را پدید آورده است، مشکلات امنیتی جدید و منحصر به فردی در این حوزه ایجاد شده که نیازمند بررسی و واکاوی است. فناوری اطلاعات و سایبر در شیوه افعال و اقدامات روزمره ما تاثیر می گذارد. برخی از مفاهیمی که در حوزه فلسفه اخلاق و فلسفه سیاسی کاربردی خاص داشته اند با پیشرفت فناوری اطلاعات دچار چالش هایی شده اند که از آن جمله می توان به مفاهیم مالکیت، حریم خصوصی، توزیع قدرت، آزادی های اساسی و مفهوم مسئولیت اخلاقی اشاره کرد. متخصصان امور رایانه چه مسئولیت های اخلاقی دارند؟ اگر یک نرم افزار کامپیوتری دچار خطا شود چه کسی مسئول است؟ آیا ایجاد اختلال در برنامه ها و ارتباطات شبکه ای کاری غیر اخلاقی است؟ آیا کپی برداری از برنامه ها و نرم افزارها در صورت عدم اطلاع و رضایت صاحبان و پدید آورندگان آنها امری اخلاقی و متعارف است؟ اینها بخشی از پرسش هایی است که در حوزه اخلاق فردی و نهادی فناوری اطلاعات مطرح می شود. با توجه به امکان دسترسی افراد مختلف به اطلاعات موجود در کامپیوترهایی که به شبکه متصل هستند؛ دولت ها، جوامع بشری، متخصصین IT و کاربران فناوری اطلاعات موظف به رعایت چه اصول اخلاقی، سیاست ها و عملیاتی در خصوص حفظ حریم خصوصی افراد می باشند؟ آینده ها و مخاطراتی از این قبیل موجب شده تا مسئله ای با نام پدافند غیرعامل در حوزه سایبر با دقت بیشتری مورد واکاوی و توجه قرار گیرد. در عصر فناوری اطلاعات و تکنولوژی ارتباطات، اشخاص با هویت های مجازی در فضای الکترونیکی حاضر می شوند و با یکدیگر گفتگو می کنند و به تبادل اطلاعات درست یا اشتباه می پردازند و گاهی غافل می شوند که ممکن است با کسی ارتباط دارند که هویتی کاملاً مخالف با آنچه نشان داده است را دارد. این یک هویت مجازی است، هویتی که البته کاربردهای خاص خود را در محیط

الکترونیک دارد و می تواند کارآمدی خاص خود را نیز داشته باشد. اما این هویت مجازی می تواند در راستای پیشبرد اهدافی شوم و ضد اخلاقی قرار گیرد. بارزترین مصداق ظهور ناهنجاری های اخلاقی و امنیتی فناوری اطلاعات، استفاده نادرست و کنترل نشده کودکان از اینترنت است. موارد مشابه گمراهی و به خطر افتادن آنها توسط سودجویان اینترنتی است که هر چند وقت یکبار اخبار نگران کننده ای در این رابطه از رسانه ها منتشر می شود. بنابراین زندگی مجازی و دنیای دیجیتال ارتباطات دارای هنجارهای رفتاری هستند که باید به آنها توجه نمود و لازم است آنها را به عنوان مسائل اخلاقی و اجتماعی رعایت کرد.

اخلاق رسانه ای و اطلاع رسانی

همانطور که کاربران، متخصصان و تولید کنندگان علم و فناوری ملزم به رعایت اخلاق علمی و فناوری هستند، رسانه ها و پایگاه های خبری و اطلاع رسانی نیز از این قاعده مستثنی نیستند. از مهمترین وظایف یک پایگاه خبری و رسانه ای که به عنوان منبع اطلاع رسانی در جامعه فعالیت می کند، رعایت حدود اخلاقی و انعکاس حقایق و واقعیت ها است. اخلاق رسانه ای در افکار عمومی جامعه نقش بسزایی در تامین امنیت اجتماعی سایبر دارد و یکی از جنبه های مهم پدافندی دنیای مجازی^۱ می باشد. پیشرفت فناوری و در راستای توسعه وسایل ارتباطی و اطلاعاتی که رابطه ای مستقیم با جامعه دارند و بر افکار عمومی موثر هستند، بیانگر اهمیت آن در تمامی ابعاد جامعه جهانی است و قرن حاضر عصر تبادل اطلاعات است. بنابراین امروزه کشورها برای دستیابی به اهداف و منافع خود در سایر نقاط جهان از این فناوری ها بهره های فراوانی می برند. وزارت ارتباطات و فناوری اطلاعات، سازمان نظام صنفی رایانه ای کشور، دانشگاه ها و

^۱ Virtual World

مراکز آموزش عالی و نیروی انتظامی جمهوری اسلامی ایران به عنوان عرضه کنندگان و تبیین کنندگان سیاست کلی فناوری اطلاعات در کشور نقش اساسی در تعیین جایگاه اخلاق و مسائل اخلاقی کاربران و تاثیرات آن در جامعه را دارند. تاکنون سازمان ها و نهادهای مرتبط با فناوری اطلاعات و ارتباطات تنها نقش مجری و نظارت کننده بر عملکرد بخش های مختلف ارتباطی و کنترل دسترسی کاربران را ایفا نموده اند که این عملکرد کافی نیست. مهمترین، تاثیرگذارترین و اساسی ترین اقدام تبیین خط مفروض ها و رعایت نکات اخلاقی و تضمین سلامت دیجیتالی جامعه، آموزش همگانی بصورت جامع و فراگیر است. آموزش باید از طریق رسانه های جمعی همچون: صدا و سیما، مطبوعات، معاونت اجتماعی نیروی انتظامی، برگزاری جشنواره ها و همایش های عمومی در سطح جامعه و در لایه های بالاتر و در سطح دانشگاهی و آکادمیک بصورت تخصصی انجام شود.

نقش فیلترینگ و کنترل دسترسی در تامین امنیت رسانه و ارتباطات

مدتی است که در کشور سیاست فیلترینگ^۱ یا فیلتر کردن برخی از سایت ها اجرا شده است و هدف آن منع استفاده از سایت های غیر اخلاقی و محتوای سایت های انحرافی سیاسی برای کاربران بوده است. البته یکی از نگرانی های سیاستگذاران فیلترینگ و کنترل دسترسی در جامعه، استفاده نادرست و انحرافات اخلاقی یا سیاسی و نشر اکاذیب و انتشار اخبار نادرست سیاسی بر علیه نظام مقدس جمهوری اسلامی ایران و هویت اصیل ایرانی - اسلامی مردم ایران است. به همین منظور در حوزه کنترل دسترسی به شبکه جهانی اینترنت و رسانه های ارتباطی و فناوری اطلاعات، سیستم فیلترینگ راه اندازی شده است. این سیستم به نحوی طراحی شده که محتویات

^۱ Filtering

اینترنت را کنترل نمایند و مطالب تعریف شده را در لیست صفحات سیاه و غیرمجاز قرار دهد.^۱ از این فیلترها می‌توان برای منع دسترسی به سایت‌های ضد اخلاقی، انحرافات سیاسی، خشونت بار، نمایش دهنده مواد مخدر و تبلیغ کننده مشروبات الکلی استفاده کرد. از طرفی نیز می‌توان از فناوری اطلاعات و ابزار اینترنت برای انتشار ذخایر غنی فرهنگی و ادبی ایران و گسترش علوم در جهان استفاده نمود و از آن برای آموزش و پرورش، تجارت الکترونیک، بانکداری الکترونیک، اطلاع رسانی، خدمات رسانی به مردم در دولت الکترونیکی، تبلیغات، مسایل و آموزه های مذهبی و دینی و توسعه ارتباطات بین الملل و صلح جهانی و ارتقای بلوغ فکری و بصیرت سیاسی و فرهنگ سازی اسلامی استفاده کرد. اخلاق در فناوری اطلاعات و سلامت دیجیتالی یک زمینه نوظهور از برخورد انفورماتیک، بهداشت روانی و ارتباطات در عصر اطلاعات است که از طریق شبکه جهانی اینترنت و تکنولوژی های مرتبط با آن ارتقا و تکامل می یابد. با توجه به آماج حملات تبلیغاتی و ضد هویتی غرب در فضای سایبر و رسانه ها، حفظ ارزش های هویت دینی و ملی ضرورت بسیاری دارد. اینترنت و ابزار فناوری اطلاعات با تمامی جذابیت ها و محبوبیت خود، دنیای مجازی جهت تبلیغات ضد هویتی برای جوانان مسلمان ایرانی به شمار می آید. آگاهی از اهداف و سوء نیت ها در تبلیغات گروه های انحرافی و التزام به آگاهی حفظ امنیت کاربری در شبکه جهانی وب از نکات مهم و ضروری کاربران فناوری اطلاعات خصوصاً نسل جوان است. با مطالعات انجام شده مشخص گردید ۷۰٪ کاربران به راحتی می توانند از سد فیلتر و کنترل دسترسی اعمال شده بر روی سایت های فیلتر شده عبور کرده و به مطالب مخرب موجود در اینترنت دسترسی پیدا کنند. جلوگیری از دسترسی به مطالب غیر اخلاقی و ضد هویتی که در جهت بهره برداری ضد ایرانی و اسلامی و ادامه تهاجم فرهنگی دشمنان در سطح وسیع و گسترده ای از شبکه اینترنت و ماهواره های بیگانه

۱ تاملی بر فیلترینگ، مرکز پژوهش های مجلس شورای اسلامی، دفتر مطالعات و فناوری های نوین. خرداد ۱۳۸۶

منتشر می شود، با اعمال تنها یک روش فیلترینگ و کنترل دسترسی امکان پذیر نمی باشد. لذا می باید در زمینه فرهنگ سازی نیز سرمایه گذاری شود تا کاربران اینترنت با آگاهی و بصیرت سیاسی و اجتماعی بیشتری از منابع و امکانات موجود در فناوری اطلاعات استفاده کنند و ضریب تهدیدات نرم توسط دشمنان در سایبر، رسانه های ارتباط جمعی و ماهواره کاهش پیدا کند. از مهمترین و موثرترین متولیان امر فرهنگ سازی کاربری فناوری اطلاعات می توان به نیروی انتظامی اشاره کرد و از آن به عنوان یک رکن فرهنگ سازی در بطن جامعه نام برد.

مخاطبان اصلی و اهداف حملات سایبری

بحران وارده گاهی بر مخاطبان خاصی وارد می شوند تا تاثیر عمیق تری را در ریشه نظام اجتماعی یک جامعه وارد کنند. از آن جمله می توان تاثیر پذیرترین نوع مخاطبان در یک جامعه را نسل جوان آن نظام دانست که آینده سازان و پشتوانه های علمی، فرهنگی و اجتماعی آن نظام هستند. در واقع شروع بحران در سطح جوانان عواقب و پیامدهای مخرب زیر را با خود به همراه خواهد داشت. عواملی نظیر:

- خود باختگی فرهنگی
- کاهش عزم در اندیشه ملی
- عدم امید به آینده
- فراموشی فرهنگ حفاظت از کیان و حفظ ارزش های سیاسی و جغرافیایی کشور
- ترس از آینده شغلی و اجتماعی

آسیب ها و تهدیدات سایبری در ایران دارای ابعاد گوناگون و بسیار وسیعی است که برخی از آن عبارتند از :

- ابعاد اجتماعی

موارد زیر از جمله تهدیدات و آسیب های فناوری اطلاعات در ابعاد اجتماعی است :

۱. **ارتباطات نامتعارف در بین جوانان:** اینترنت و فضای سایبر به دلیل تسهیل ایجاد روابط دوستانه در زمینه های غیر اخلاقی بسیار مورد توجه قرار گرفته و موجب سهولت خیانت در روابط زناشویی و ایجاد روابط نامشروع می شود. حتی فضای سایبر تمامی کاربران و به ویژه جوانان را قادر می سازد به آسانی به اعمال غیر اخلاقی مانند قمار بازی و یا شرکت در شرط بندی های مجازی بپردازند.
۲. **سرگرمی های مجازی:** علاقه جوانان به مشارکت اجتماعی و فعالیت های مدنی را با انگیزه های مختلف تحت الشعاع قرار می دهد و می تواند بر مهارت های اجتماعی آنان در تدارک فراغت های گروهی و تفریحات و بازی ها غیر مجازی تاثیر منفی بگذارد. مطالعات نشان می دهد مردان در اینترنت به دنبال راه هایی برای کسب قدرت و شهوت و همین طور تحقق رویاهای جنسی هستند و زنان بیشتر به دنبال گروه های دوستی و حمایت روابط عاشقانه می روند. روابط غیر اخلاقی تنها در فضای سایبر باقی نمی ماند و در بسیاری موارد به روابط فیزیکی می انجامد.
۳. **جرایم رایانه ای و سایبری:** شاید نفوذ به سایت بانک ملی ایران و شبکه شتاب یکی از مهم ترین نشانه های آسیب پذیری جامعه ایرانی از اینترنت است و البته گسترده بودن تعداد سایت های آموزش نفوذ یا هک و بالا بودن تعداد نفوذ کننده ها^۱ و آمار بالای سایت های هک شده، حکایت از رسوخ بیشتر این پدیده به جامعه دارد. گسترش شبکه های مجازی تجارت

^۱ Hacker

الکترونیک و آن چه به نام گلدکوئیست و پنتاگون و چند نام دیگر شناخته شده است، آسیب پذیری فضای سایبری را در این زمینه نشان می دهد.

۴. گسستن میان نسلی: اینترنت شکاف میان نسلها را آشکارتر ساخته است. اکنون نه تنها شکاف میان نسل اول و دوم متمایل به سایبر بلکه شکاف میان نسل دوم و سوم علاقه مند به اینترنت نیز پدیدار شده، به گونه‌ای که هیچ یک زبان دیگری را نمی فهمند و یا کمتر به زبان هم حرف می زنند.

۵. بی هویت سازی: با امکانات و گزینه‌های فراوانی که اینترنت در اختیار جوانان می‌گذارد آنان به طور دائم با این فضا، هویت نامشخص و اغلب متحولی را می‌آفرینند، یعنی اینترنت یک صحنه اجتماعی است که فرد خود را در موقعیت‌های متنوع نقش‌ها و سبک‌های زندگی، قرار می‌دهد و از آن تاثیر می‌پذیرد. نوجوانان در صحنه اینترنت برای ایفای هر نقشی، فرصت پیدا می‌کنند. اینترنت فضای آزاد گلخانه‌ای را ایجاد می‌کند که حتی معلمان و مراجع قدرت به آن دسترسی ندارند و بر آن تاثیر نمی‌گذارند. امکان خصوصی بودن امور در سایبر، نکته‌ای است که کاربران جوان اینترنت به آن علاقه دارند.

۶. تهدید بنیان‌های خانواده: تغییر ارزش‌ها و هنجارهای اجتماعی به نوبه خود بنیان‌های خانوادگی را در معرض تهدید قرار می‌دهد.

۷. اعتیاد الکترونیکی: توان اعتیاد آورنده مواد مخدر براساس سرعت جذب مواد مزبور به بدن انسان است، اما در مورد سایبر و اینترنت این سرعت به میزان در دسترس بودن آن است که ایجاد اعتیاد می‌کند. افزایش سرعت مودم‌ها و سهولت دسترسی به شبکه‌ها، سطوح بالاتری از استفاده اعتیادآمیز اینترنت را دامن می‌زند، اعتیاد به اینترنت مثل هر نوع اعتیاد دیگری، یک بیماری اجتماعی است. لذا پدیده‌ای است فراگیر که با صدمات روانی و اجتماعی، خانوادگی،

جسمانی و حتی اقتصادی همراه است. معتادان به اینترنت مانند اغلب انواع معتادان، دچار افت در کارکردهای فردی و اجتماعی می‌شوند، اما فرق این اعتیاد با سایر این است که معتادان اینترنت کمتر احساس گناه می‌کنند. این افراد، اغلب جزو افراد تحصیل کرده و با فرهنگ جامعه هستند، اگر چه هنوز معیاری برای تشخیص اعتیاد به اینترنت ارایه نشده است، ولی علایم این نوع اعتیاد را به دو دسته علایم روانی و جسمانی تقسیم کرده‌اند. علایم روانی عبارتند از: نوعی احساس لذت و رضایت هنگام دسترسی به اینترنت و ناتوانی در متوقف کردن افسردگی و بدخلقی در مواقعی که دسترسی به اینترنت وجود ندارد و دروغ گفتن به دیگران در مورد میزان استفاده از اینترنت و علایم جسمی عبارتند از: علایمی ناشی از نشستن زیاد است (سوزش چشم و سردرد و کمر درد و اضافه وزن و بی نظمی در غذا خوردن و صرف نظر کردن از بعضی وعده های غذایی و توجه نکردن به بهداشت و آراستگی فردی و اختلالات خواب و تغییر در الگوی خواب).

۸. شکل گیری خرده فرهنگ‌های مختلف: کارکرد غالب چت‌های اینترنتی در جوانان ایرانی از جنبه های فراغتی و سرگرم کننده آن است. نتایج یک تحقیق بیانگر این است که فضای غالب در محیط چت، مورد مراجعه جوانان، گفتگوهای دوستانه جوانان غیر هم جنس است که با نیت ارضای کنجکاوی، آشنایی و سرگرمی و گاه ماجراجویی بدان روی می آورند. سرگرمی‌های مجازی، علاقه جوانان به مشارکت اجتماعی و فعالیت‌های مدنی را با انگیزه‌های مختلف تحت الشعاع قرار می‌دهد و می‌تواند بر مهارت های اجتماعی آنان در تدارک فراغت های گروهی و تفریحات و بازی های غیر مجازی تاثیر منفی بگذارد. هم چنین مجاورت طولانی با فضای مجازی می‌تواند به فرهنگ پذیری یک طرفه تاثیرپذیری افراطی از هنجارها و ارزش ها در

عرصه های مختلف ارتباطی و اجتماعی انجامیده و با تقویت جهان وطنی، تعلقات ملی و سنتی کاربران را تحت تاثیر قرار دهد.

۹. انتشار مطالبات قومی منطقه‌ای و افزایش تحریک‌پذیری قومیت‌ها: خاصیت تاسیس

سایت های قومی و راه اندازی وبلاگ های منطقه ای و انتشار برخی مطالب تحریک آمیز در سایت های اینترنتی، قابلیت این رسانه و پدیده برای دامن زدن به مباحث مناقشه برانگیز قومی را بالا برده است.

- ابعاد فرهنگی

۱. کاهش نفوذ رسانه‌های ملی و داخلی: به همان اندازه که رسانه‌های خارجی و رسانه‌های اینترنتی مخاطب جدید کسب می‌کنند از تعداد مخاطبان رسانه‌های داخلی و ملی و میزان نفوذ آنها کاسته شده است.

۲. ایجاد محرکه‌های قوی برای تبادلات فرهنگی غیر قابل کنترل: با وجود اینترنت بسیاری از محصولات فرهنگی که ماده اولیه آنها اطلاعات است مثل کتاب، مقاله، موسیقی، فیلم، نقاشی و عکس به راحتی و بدون مانع مبادله می‌شوند. این بهم آمیختگی فرهنگی به ویژه میان ایرانیان داخل و خارج کشور غیر قابل کنترل شده است.

۳. بستر سازی بیشتر برای تهاجم فرهنگی: رسانه اینترنت به همه سرویس های متنوعش، قابلیت تبدیل شدن به بستری برای تهاجم فرهنگی را دارد.

۴. **انتقال ناهنجاری های ارزشی و اخلاقی غربی:** اینترنت یک پدیده غربی است و فرهنگ حامل آن نیز غربی است، پس چندان غیر معقول نیست اگر بگوییم اینترنت موجب انتقال هنجارها و ناهنجاری های ارزشی و اخلاقی غربی می شود.

۵. **چالش های انتقادی در مباحث دینی و مذهبی:** قبح زدایی از برخی مباحث و قداست شکنی از بسیاری مباحث دینی و مذهبی با انجام شدیدترین حملات به اصول مبانی اسلامی با استفاده از فضای سایبری صورت پذیرفته است.

۶. **جایگزینی رسانه های:** با وجود اینترنت و سایبر تمرکز سیستم رسانه های کشور از دست رسانه های داخلی خارج شده و خلاء موجود را رسانه های سایبری پر می کند. بازی های رایانه ای ایزاری است که از طریق اینترنت قابل دریافت و ارسال است. بازی های اینترنتی اگر از محتوای تهاجمی برخوردار باشد، آسیب های فراوانی به همراه دارد. آسیب های فیزیولوژیک بازی ها بیش از سی میلیون نفر در سراسر جهان، بخشی اوقات فراغت خود را با بازی های رایانه ای پر می کنند که بالغ بر ده درصد آنها بین چهار تا هفت ساعت از زندگی روزمره شان را به بازی با رایانه اختصاص دادند. طی تحقیقات انجام شده، بازی ها، ضربان قلب و میزان هورمون های بدن را تغییر می دهد. افرادی که به طور فعال در بازی ها شرکت نمی کنند، فشارهای عصبی زیادی را تحمل می کنند. محققان به این نتیجه رسیده اند که تاثیرات روحی و روانی بازی های رایانه ای بسیار شبیه به بازی های حقیقی و ورزش های پر استرس است. حس کاربری که شکست می خورد و فشارهای روحی که او متحمل می شود، بسیار شبیه به حس بازیکنان شکست خورده فوتبال است و تاثیرات روانی این بازی ها بسیار به هم شبیه است.

در مجموع علت این اهمیت بازی های رایانه ای توانایی آنها در انتقال پیام های فرهنگی، مذهبی و سیاسی است. القای معانی از طریق بازی بسیار بیشتر از فیلم و کتب و نشریه است، زیرا کاربر خود را به جای قهرمان بازی می بیند که غالباً این قهرمان، غربی یا آمریکایی است. علم روانشناسی ثابت کرده است برخی از دروغ ها اگر بسیار تکرار شوند تاثیر خود را گذاشته و سبب انحراف فکری می شود. در نتیجه بازی هایی که ضد مهدویت هستند، می تواند سبب انحراف اعتقادات آخرالزمانی کاربر شوند. پس می بینیم که بازی رایانه ای می تواند ابزاری باشد برای جنگ با اعتقادات دینی، مذهبی و اسلامی. مواردی که به آن اشاره شد به عنوان تهدیدات فناوری اطلاعات و دنیای سایبر اطلاق می گردد. چنین عملیاتی بطور مشخص با اهداف تهدید امنیت و یا حفظ امنیت در ابعاد ملی انجام می پذیرد. تهدیدات و آسیب های اجتماعی فناوری اطلاعات دارای اهمیت روزافزون برای بخش های انتظامی و امنیتی، اقتصادی و تجاری، سیاسی، فرهنگی، اجتماعی است. لازمه داشتن یک محیط سالم و پلیس مقتدر در فضای سایبر، همانا ارتقاء سطح آموزش خانواده ها، مدارس و دانشگاه ها و بالا بردن سطح امنیتی عناصر درگیر در این فناوری است و این مهم جز با افزایش دانش در حوزه سایبر میسر نخواهد بود. پس لازم است ابتدا به فرهنگ سازی و آموزش در جامعه پرداخته شود و سپس به کشف جرم و یا مقابله با تهدیدات موجود در فناوری اطلاعات و رسانه ها.

نتیجه گیری و پیشنهادات

توسعه علوم رایانه و فناوری اطلاعات و ارتباطات تمامی علوم موجود در جهان را تحت تاثیر خود قرار داده است. همچنین هر جامعه ای برای جلوگیری از عقب ماندگی علمی و تکنولوژیک به ناچار باید با پیشرفت علوم و فناوری همگام و همراه شود. با توجه به آماج حملات فرهنگی و تهدیدات فناوری اطلاعات و شبکه اینترنت در زمینه های مختلف اجتماعی، فرهنگی، اخلاقی، سیاسی، علمی و تعداد بسیار زیاد کاربران ایرانی در اینترنت در راستای تاثیرگذاری بیشتر و کاهش هزینه های فیلترینگ و کنترل دسترسی برای مقابله با تهدیدات سایبری و آفندهای اجتماعی آن، پیشنهاد می گردد نیروی انتظامی جمهوری اسلامی ایران با هدایت منابع و امکانات موجود در جهت افزایش سطح آگاهی و بلوغ فکری کاربران و فرهنگ سازی (مهندسی فرهنگی) پایه های امنیت اجتماعی سایبری را مستحکم نماید. همچنین پیشنهاد می گردد مدلی کاربردی از سطوح مختلف کاربری اینترنت توسط کاربران جهت کنترل دسترسی و فرهنگ سازی در مقابل تهدیدات اینترنت و فناوری اطلاعات تهیه و به اجرا گذاشته شود که این مدل شامل کاربران:

۱- سطح یک (اساتید دانشگاه، مدیران ارشد، نخبگان و پژوهشگران)

۲- سطح دو (دانشجویان، دانش پژوهان و دانش آموزان)

۳- سطح سه (کاربران عمومی فناوری اطلاعات) باشد تا به تناسب نیاز و بصیرت و آگاهی

سیاسی هر سطح در زمینه فرهنگ استفاده از رسانه و ارتباطات، تشخیص مطالب واقعی

و غیر واقعی و توانمند سازی در مقابله با تهدیدات موجود فرهنگ سازی شود.

پیشنهاد می شود به منظور رعایت سلامت سایبری و اخلاقی، یک گروه دیده بان سایبری متشکل از نیروهای متخصص پلیس به عنوان بخشی از تلاش های جاری برای مصون نگاه داشتن کودکان در شبکه جهانی اینترنت، به طور سیستماتیک راه اندازی گردد. همچنین با استفاده از فیلترینگ و

کنترل دسترسی سایبری می‌توان برای منع دسترسی کاربران به سایت‌های خشونت بار، نمایش دهنده مواد مخدر و تبلیغ کننده مشروبات الکلی استفاده کرد. برای ارتقاء امنیت اجتماعی سایبر، توجه به اخلاق حرفه ای به دلیل این که متخصصان تنها با تسلط بر کار و فعالیت حرفه ای خود و فلسفه و نقش آن در زندگی مردم، به درک اخلاقی نایل می آیند و عینیت گرایی و بی طرفی علمی و عدم جانبداری سیاسی که مهمترین اصل اساسی علم و فناوری است، در رابطه با اخلاق علمی حرفه ای لازم و ضروری است. در ادامه به راهبردهای اصلی مقابله با تهدیدات و آسیب های سایبری و مخاطرات امنیت اجتماعی اشاره می شود:

۱. نهادینه سازی رعایت قانون جرائم رایانه ای مصوب مجلس شورای اسلامی.
۲. ساماندهی، انسجام بخشی و هدایت راهبردی مجموعه های علمی، پژوهشی، آموزشی، انتظامی و امنیتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فناوری های بومی و ملی مورد نیاز برای مقابله با تهدیدات فناوری اطلاعات و ارتباطات.
۳. توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری های بومی و استفاده از پلیس متخصص سایبری.
۴. حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مولفه های امنیت، ایمنی، پایداری و متکی بر فناوری های بومی.

فهرست منابع

- سوری، جواد (۱۳۸۷). نقش فناوری‌های نوین ارتباطی در عملیات روانی، فصلنامه عملیات روانی، شماره ۱۲.
- مانوئل کاستلز، (۱۳۸۰). ترجمه: احمد علیقلیان و افشین خاکباز، عصر اطلاعات و ظهور جامعه شبکه‌ای، انتشارات طرح نو.
- دیلمقانی، میترا و، حجازی، سید علیرضا (۱۳۸۶). تأثیر سازنده اینترنت بر اخلاق کاربران عصر فناوری اطلاعات.
- پدافند غیرعامل در حوزه جنگ سایبر، شرکت ایز ایران، مرکز پدافند غیرعامل.
- از مدیریت بحران تا هدایت رسانه در جنگ نرم، سازمان پدافند غیرعامل.
- تأملی بر فیلترینگ (۱). اقدام پیشگیرانه از جرائم رایانه‌ای، دفتر مطالعات ارتباطات و فناوری های نوین (۱۳۸۶). مرکز پژوهش‌های مجلس شورای اسلامی.
- مجیدی، عبد... . نقش رسانه‌ای اینترنت در ناامنی‌های اجتماعی.
- جمعی از نویسندگان (۱۳۸۵). نقش فناوری اطلاعات در جنگ‌های آینده، موسسه آموزشی و تحقیقاتی صنایع دفاعی.
- گروه تحقیق (۱۳۸۴). جهانی شدن ارتباطات و تهدیدهای امنیت ملی ما، فصلنامه راهبرد، شماره ۳۶.
- جهانگرد، نصر... و سلجوقی، خسرو (۱۳۸۳). مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات ایران، دبیرخانه شورای عالی اطلاع‌رسانی.
- اظهارنظر کارشناسی درباره لایحه پیشگیری از وقوع جرم (۱۳۸۵). مرکز پژوهش‌های مجلس شورای اسلامی، شماره ۷۸۹۱.

- Lee, P, Y, (2003), Structural and Content-based Analysis for Web Filtering, Internet research: electronic networking applications and policy, Vol13, No . 1, pp.27-37.
- Shinder, Debar Littlejohn, Scene of the Cyber Crime, Computer Forensics Hand Book, Syngress Publication, 2002.

