امنیت انسانی و کاربرد فناوری های نوین اطلاعاتی و ارتباطی

دکتر محسن آیتی* و سید علیرضا محمدزاده**

چکیده:

در سه دهه ی اخیر توسعه ی تکنولوژی خصوصاً در زمینه های ارتباطی باعث افزایش ارتباطات در جوامع انسانی شده است. تحول در حوزه های ارتباطی مرهون پیشرفت های خیره کننده بشر در حوزه های علوم کامپیوتر و سخت افزار و نرم افزار و دانش فناوری اطلاعات و ارتباطات است. ارتباطات نوین و تجهیزات ارتباطی ماهواره ای و اینترنت مرزهای جغرافیایی را کم رنگ کرده و ارتباطات انسانی و فرهنگی جدیدی را به جوامع انسانی تقدیم نموده است. این پیشرفت ها در علوم و تکنولوژی هر چند تسهیلات فراوانی برای بشر فراهم آورده است، در عین حال باعث ایجاد مشکلات جدیدی برای بشریت شده است. از جمله این مشکلات می توان به تضعیف روابط عاطفی و انسانی و ناهنجاری های اخلاقی و اجتماعی و فرهنگی اشاره کرد. از سوی دیگر برخی را اعتقاد بر آن است که همگرایی تکنولوژی در جوامع انسانی می بایست باعث تقویت امنیت انسانی در کشورها و رشد و تقویت اخلاق و فرهنگ شود. هر چند میزان این همگرایی در جوامع مختلف متفاوت است. امروزه بسیاری از مردم از شبکه های اینترنت یا اینترانت برای مبادله پیام یا فعالیت های دیگر استفاده می کنند. این فناوری فاصله های زمانی و مکانی را از بین برده است و قدرت زیادی را در اختیار بشر قرار داده است. اگرچه این فناوری باعث تسهیل ارتباطات و پیشرفت های گسترده شده است، اما فضایی را برای سوء استفاده افراد بزهکار برای بر هم زدن امنیت انسانی از طریق سوء استفاده های اطلاعاتی، تخریب اطلاعات و نا امن کردن فضای زندگی و کاری انسانها بوجود آورده است. نفوذ گران به شبکه های کامپیوتری اهداف مختلفی را دنبال می کنند که جنبه های مختلفی از زندگی انسانها همانند اهداف سیاسی، اقتصادی، امنیتی، اجتماعی و ... را مورد هجمه قرار می دهد. از این

* استادیار، گروه علوم تربیتی دانشگاه بیرجند. پست الکترونیکی: ayati_mohsen@yahoo.com

** عضو هیأت علمی گروه کامپیوتر دانشگاه پیام نور خراسان جنوبی: mohamadzaeh@pnu.ac.ir

رو به نظر می‌رسد این فناوری‌ها نیازمند اعمال مدیریت برای مقابله با تهدیدات ذکر شده است. مدیریتی که می بایست هم در جنبه های فنی، سیستمی و نرم افزاری و هم در سایر جنبه های نظارتی بطور فعالانه وارد صحنه شود و نظام جدیدی از طراحی و کاربرد را برای فناوریهای نوین تعریف نماید .

در این مقاله سعی شده است ضمن شناسایی ابعاد مختلف امنیت در سطوح مختلف و تعریف آن، چگونگی بر هم خورد امنیت انسانی در اثر پیشرفت های نوین و فناوری های جدید تبیین و در ادامه راهکارهای مقابله با این تهدیدات امنیتی از جهات مختلف مورد بررسی قرار گیرد .

واژه های کلیدی: *امنیت انسانی، فناوری اطلاعات و ارتباطات ، مدیریت فناوری*

مقدمه

امنیت نیز مثل هر مقوله ذهنی و اجتماعی دیگر در جهان دستخوش تغییر و دگرگونی شده است. عوامل و متغیرهای امنیت زدا در دنیایی که اطلاعات و ارتباطات مرزهای آن ها را در هم شکسته است، از نو تعریف می شود. امنیت در جهان واقعی چه در مقیاس فردی و چه در مقیاس اجتماعی آن، مفهومی پویاست که تحت تاثیر فرصت ها و تهدیدهای جدید ملی و بین المللی تبیین و تفسیر می شود .

وابستگی متقابل کشورها که بیشتر به سبب حاکمیت ساختارهای نظام سرمایه داری و پیشرفت فناوری اطلاعات و ارتباطات است، از مهم ترین پیامدهای جهانی شدن است . این پدیده ضمن نفوذ پذیر ساختن مرزهای جغرافیایی کشورها جنبه های حاکمیت را به ویژه در کشورهای در حال توسعه به چالش کشیده است. از آنجا که برای بسیاری از کشورهای در حال توسعه استقلال سیاسی و تمامیت ارضی ارزش های ملی حیاتی و سرنوشت ساز است، هر گونه تهدید این ارزش ها نگرانی های امنیتی را در پی خواهد داشت. دسترسی به نظام اطلاعاتی تنها با یک کامپیوتر و خط ارتباطی میسر است، بنابراین در چنین نظامی هر تراشه یا چیپ یک تهدید و هر کامپیوتر یک سلاح بالقوه خواهد بود. چنین سلاح هایی می تواند توسط هر کس حتی آنهایی که آشنایی مختصری با کامپیوتر دارند به کارگیری شود(فتحیان ۱۳۸۶).

اطلاعات توسط منابع مختلف تولید، در محل های انباشت مناسب ذخیره می شود، سپس پردازشهای لازم انجام شده و برای انتقال به محل‌های دیگر از بستر ارتباطی عمومی استفاده می شود. چنین چرخه ای مبین یک نظام اطلاعاتی است که اجزای اصلی

آن، اطلاعات، سخت افزار، نرم افزار، وسایل ارتباطی و انسان است. اطلاعات ماده اولیه چنین نظامی است. سخت افزار در برگیرندهٔ مجموعهٔ وسایلی است که از یک سو پردازش و ذخیرهٔ اطلاعات را میسر ساخته و از سوی دیگر تعامل میان ماشین و محیط را ممکن می نماید. نرم افزار مجموعه دستوراتی است که با هدایت و برنامه ریزی انسان، پردازش داده ها و کنترل سیستم ها را بعهده دارد. شبکهٔ ارتباطی نیز امکان انتقال اطلاعات را با استفاده از پروتکل های مناسب میسر می سازد و انسان نیز استفاده کننده اصلی نظام اطلاعاتی می باشد. امروزه کشورها و افراد برای تاثیرگذاری بر ادراک دیگران به منظور متاثر کردن احساسات، تعقل و تصمیم گیری، اطلاعات را تحریف و در اختیار دیگران قرار می دهند. با فناوری‌های دیجیتال امروزی می توان به آسانی اطلاعات کاذب را جعل و یا اطلاعات موجود را تحریف کرد. اسناد را ایجاد و دستکاری نمود. نوارها را برید و به هم مونتاژ کرد. تصاویر را به شیوه ای تغییر داد که واقعی اما کاملا با اصل خود متفاوت به نظر برسند.

در حالی که رسانه ها در معرض تغییر و تحریف هستند، اکثر مردم آنچه را که در محیط فیزیکی شان می بینند و می شنوند باور می کنند. اما این نیز ممکن است در آینده در معرض تحریف قرار گیرد. عده ای عقیده دارند که تا سال ۲۰۱۵ می توان تصاویر سه بعدی با درجهٔ وضوح بالایی را در هوا ایجاد کرد. افراد و اشیاء را می توان طوری ارائه داد که گویی در محیط فیزیکی وجود دارند. در حالی که عملاً این گونه نیست. اگر چنین اتفاقی رخ دهد دیگر به چه رسانه ای می توان اعتماد کرد (من[1]، ۱۹۹۳).

جنگ اطلاعاتی

جنگ اطلاعاتی هر اقدامی است که برای انکار، سوء استفاده، تحریف یا تخریب اطلاعات و یا کارکردهای دشمن انجام می شوند، همچنین عملیات حفاظت از خود در برابر این گونه اقدامات و بهره برداری از عملیات اطلاعاتی خودی را شامل می شود. در واقع جنگ اطلاعات، به معنی نزاع بین دو یا چند دشمن برای کنترل فضای اطلاعاتی محسوب می‌شود.

جنگ اطلاعات از ویژگی های خاصی برخوردار است که از جمله می توان به مواردی همچون: به کارگیری تعداد نیروهای اندک، خاموش بودن و استفاده از تجهیزات پیشرفته اشاره کرد. چنین جنگی می تواند بصورت ذیل انجام پذیرد (فولادی، ۱۳۸۱).

- ✓ کاشتن مین های اطلاعاتی
- ✓ شناسایی اطلاعاتی

[1] Mann, Edward

- ✓ تغییر در شبکه های اطلاعاتی
- ✓ رها کردن بمب های اطلاعاتی
- ✓ حذف کردن اطلاعات زائد خودی
- ✓ انتشار شایعات
- ✓ استفاده از ترفندهای اطلاعاتی
- ✓ سازمان دهی دفاع اطلاعاتی
- ✓ پخش اطلاعات کپی شده
- ✓ تاسیس پایگاه های جاسوسی شبکه ای

جنگ اطلاعات هر نوع رسانه ای از قبیل، شبکه های مخابراتی، شبکه های کامپیوتری، وسائل ذخیره مغناطیسی، ابزارهای نوشتاری و پخش گسترده را در بر گرفته و دامنهٔ آن مواردی چون جرایم کامپیوتری، تروریسم، امنیت ملی و حقوقی فرد را شامل می شود. تروریست ها، سیستم اقتصادی، اجتماعی، نظامی و سیاسی را مورد هدف قرار می دهند. در نظر بگیرید که شخصی بتواند وارد سیستم کامپیوتری بازار بورس شده و در آن تغییراتی ایجاد کند. این تغییرات می تواند شرکت های بزرگ را به ورطه ورشکستگی بکشاند و در نهایت در کشور بحران اقتصادی ایجاد نماید. یا تصور کنید در جامعه ای که روی سامانه های خبری، خبر مرگ رهبر یک جامعه، ترور، انفجار هسته ای و غیره گذاشته شود، چه فاجعه اجتماعی رخ می دهد. در جنگ اول خلیج فارس پنج هکر هلندی وارد شبکه نظامی امریکا شدند و اطلاعات نظامی آنها را بدست آوردند. این نفوذ گران حتی قادر بودند سیستم های مدیریتی آنها را کنترل کنند و بجای موشک، مسواک به محل عملیات ارسال کنند (سلماسی زاده، ۱۳۸۰).

در کشورهای وارد کننده فناوری نظیر ایران علاوه بر تهدیدات فوق خطر بزرگ دیگری نیز وجود دارد که بسیار مهلک تر از حملات تروریست هاست. برای روشن شدن مطلب فوق در نظر بگیرید که یک سیستم فرماندهی و کنترل در سازمانهای نظامی مبتنی بر مسیر یاب های Cisco یا Tellaps ایجاد شده باشد. سازندهٔ اصلی این مسیریاب ها کشور امریکاست که ممکن است در این گونه سیستم ها " راههای نفوذی" قرار داده و با استفاده از کدهای خاص، شبکه را در موارد بحران غیرفعال کند. همان طور که FBI در جنگ اول خلیج فارس (طوفان صحرا) درون مدار مجتمع چاپگرهایی که عراق از فرانسه خریداری کرده بود، ویروسی قرار داد که قادر بود آنها را از کار بیندازد (سی. اس. پی. پی.[1]، ۲۰۰۵).

[1] CSPP

یا در نظر بگیرید که سازمانی دولتی در یک کشور سیستم امنیتی بسیار پیشرفته ای خریداری کرده که با دوربین، حتی کشوهای میز تحریر و فایلهای سازمان را کنترل می‌کند. مسئولین چنین سازمانی برای اطمینان از اینکه امکان نفوذ غیر مجاز در برنامه وجود نداردسش، کارشناسان خود را برای تحلیل عملکرد نرم افزاری سیستم به کشور سازنده اعزام می دارند غافل از اینکه امروز ریز پردازنده ها و سیستم های مخابراتی پیشرفت کرده، آنتن های فعال و جهتی امکان انتشار امواج به فواصل دور را ممکن ساخته و چنین امکاناتی به راحتی در یک دوربین قابل جاسازی است، پس اطلاعات محرمانه کشور می تواند به راحتی به کشور صاحب فناوری منتقل شود.

امنیت فناوری اطلاعات

امروزه با گسترش روز افزون کاربردهای فناوری اطلاعات موضوع تهدیدات امنیتی در این حوزه و چگونگی مقابله با آنها از اهمیت فوق العاده ای برخوردار است. استفاده از شبکه های کامپیوتری با وسعت زیاد برای تبادل اطلاعات مهم بین نقاط مختلف جغرافیایی در کنار مزایای بسیاری که برای بشر به همراه دارد عرصه گسترده ای را برای سوء استفاده پدید آورده است . بنابراین یکی از مباحث بسیار مهم در حوزه فناوری اطلاعات ، امنیت فناوری اطلاعات است . فناوری اطلاعات شامل فناوری‌هایی است که در خدمت ذخیره سازی، پردازش، انتقال و مدیریت اطلاعات است اما امنیت فناوری اطلاعات به استفاده ایمن از این فناوری و اطمینان از وجود محیطی عاری از هر گونه تهدید باز می گردد. امنیت اطلاعات را می توان در دو بخش مهم امنیت کامپیوتر و امنیت ارتباطات مورد بررسی قرار داد.

امنیت کامپیوتر: هدف از امنیت کامپیوتر نگهداری از منابع اطلاعاتی در مقابل استفاده غیرمجاز و یا نادرست و همچنین حفاظت از اطلاعات در مقابل صدمات عمدی یا غیر عمدی افشا یا تغییر است. به عبارت دیگر امنیت کامپیوتر به حفاظت از اطلاعات در طی ذخیره سازی یا پردازش آن توسط کامپیوتر که می تواند در یک شبکه قرار داشته باشد، باز می گردد.

امنیت ارتباطات: به حفاظت از اطلاعات در طی انتقال بین سیستم های کامپیوتری و شبکه ها باز می گردد.

به کارگیری فناوری اطلاعات در یک شبکه ارتباطی با خطرات امنیتی متعددی همراه است. سه مولفه ا صلی برای ارائه خدمات بر روی چنین شبکه ای شامل کاربران انسانی، ماشین ها و فرایندهای کامپیوتری است.

کاربر: موجودیتی است که در قبال فعالیتهای خود در تعامل با کامپیوتر یا شبکه ارتباطی مسئول و جوابگو است.

ماشین: موجودیتی دارای آدرس است که در یک شبکه کامپیوتری (یا سیستم توزیع شده) توسط یک نام و یک آدرس خاص در شبکه آدرس دهی می شود.

فرایند: عملیاتی است که روی ماشین ها اجرا می شود. معمولاً با استفاده از مدل مشتری کارگزار، فرایندهای سمت مشتری و کارگزار را از هم تشخیص می دهند.

هر یک از این سه عنصر ممکن است با خطرات امنیتی همراه شود و در نهایت ایجاد مشکل نماید.

نفوذ گران و اهداف حمله به شبکه های کامپیوتری

نفوذ گران افرادی هستند که با امیال و اهداف مختلف شبکه های کامپیوتری را هدف قرار می دهند. ذیلاً برخی از این اهداف مورد بررسی قرار می گیرند:

- اهداف سیاسی: نخبگان سیاسی ممکن است طعمه مناسبی باشند. نفوذگران اطلاعات آنها را تغییر داده و مطالبی را جایگزین می کنند تا شخصیت سیاسی آنها آسیب ببیند.
- اهداف تروریستی: اطلاعات سازمان های اقتصادی، امنیتی و نظامی اهداف خوبی برای تروریست ها و آن هایی که قصد دارند امنیت ملی کشورها را خدشه دار کنند، می‌باشد.
- کسب درآمد: اطلاعات ارزشمند یک مرکز ممکن است افرادی را برای سرقت و فروش آن وسوسه کند. به عنوان مثال در جنگ اول خلیج فارس چند فرد هلندی به مراکز نظامی امریکا نفوذ کرده و اطلاعات زیادی از آن بدست آوردند که قصد فروش آن را به رژیم عراق داشتند اما به علت بی اعتمادی دو طرف، معامله صورت نگرفت.
- بازی و سرگرمی: عده ای ممکن است بخاطر تفریح و سرگرمی و یا امراض روانی و کسب شهرت به شبکه ها نفوذ کنند.
- شناسایی امنیتی: نفوذ به منظور شناسایی ویژگی های امنیتی سیستم های کامپیوتری و ارزیابی نقاط ضعف را شامل می شود.
- رقابت اقتصادی: رقبای اقتصادی برای دزدیدن اطلاعات و یا از کاراندازی شبکه ممکن است به نفوذ و اختلال در شبکه اقدام کنند. در کار تجاری از کار افتادن

شبکه برای مدت زمان کمی نیز ممکن است مشتریان آنها را به شرکت رقیب هدایت کند (ملکیان، ۱۳۸۱).

دسته بندی تهدیدات امنیتی

هر عملی که امنیت اطلاعات را به مخاطره افکند، تهدید امنیتی محسوب می شود. تهدیدات یا حملات را می توان در دو دسته کلی قرار داد: تهدیدات غیر فعال، تهدیدات فعال. در تهدیدات غیر فعال اطلاعات به صورت غیر مجاز دریافت شده و تغییر مشهودی شبیه حذف یا تکرار و غیره در آن مشاهده نمی شود. به عبارت بهتر استراق سمع انجام می‌پذیرد . بدین ترتیب اطلاعات از منبع به سوی مقصد منتقل می شود و مزاحم به شیوه غیرفعال سیستم را غیرفعال می کند.

به عنوان مثال زمانی که این تهدید از طریق کشف کلید رمز اطلاعات و بهره برداری غیرمجاز از اطلاعات و یا از طریق تحلیل ترافیک اطلاعات صورت پذیرد. ردیابی چنین تهدیداتی به علت عدم تغییر در اطلاعات مشکل است. برای جلوگیری از چنین تهدیدی باید به گونه ای پیام را محرمانه نمود تا دشمن امکان بهره برداری از آن را نداشته باشد و کلید رمز پیام را نیز از دسترس دشمن محافظت نمود.

تهدیدات فعال همراه با حذف، اضافه، تکرار و به طور کلی تغییر در اطلاعات ارسالی است. در این نوع تهدید موضوع بررسی اعتبار یا صحت پیام مهم خواهد بود. برای جلوگیری از تهدیدات فعال و غیر فعال می توان از رمز گذاری پیغام به کمک یک کلید ساده استفاده کرد به گونه ای که پیغام از کانال ناامن ولی کلید از کانال یا محیطی امن منتقل گردد.

دسته بندی نفوذ گران از حیث رفتاری

با توجه به اهداف پیش گفته، نفوذگران در شبکه های کامپیوتری به چند دسته ذیل تقسیم می شوند:

- " هکر ": شخصی است که از مهارت زیاد در زمینه برنامه نویسی و شبکه های کامپیوتری برخوردار بوده و به منظور شناسایی ویژگی های امنیتی سیستم های کامپیوتری در آنها رخنه می کند لیکن نقش تخریبی ندارد.
- " کراکر ": شخصی است که برای بهره برداری غیرمجاز، سرقت و یا تخریب اطلاعات در سیستم های کامپیوتری نفوذ می نمایند.

- " واکر ": نفوذ گران مزاحمی را گویند که شبیه کراکر ها در پی خرابه کاری یا سرقت اطلاعات نمی باشند.

دسته بندی نفوذ گران از حیث شخصیتی

آشنایی با هویت نفوذ گران برای مقابله با آنان بسیار مفید است. نفوذ گران را می توان از جهت شخصیتی به صورت زیر دسته بندی نمود:

۱. نفوذ گرانی که تنها هدفشان سرگرمی و شهرت است. آنها این کار را انجام می‌دهند تا وقت خود را پر کرده و به شهرت دست یابند.
۲. خراب کاران که هدفشان آسیب رسانی به سیستم ها و اطلاعات ذخیره شده در آنها است. آنها مشکلات بزرگی را به بار می آورند، اما خوشبختانه تعداد آنها کم است.
۳. برخی از نفوذگران، کارمندان اخراجی هستند که به سیستم های سازمان دسترسی داشته اند و لذا از اطلاعات مفیدی برای نفوذ برخوردارند.
۴. خیلی از افرادی که به کامپیوترها نفوذ می کنند همه اطلاعات را نمی دزدند بلکه اطلاعاتی را که قابل تبدیل به پول بوده و یا رای دسترسی به آینده استفاده می شود را می ربایند.
۵. خیلی از حوادث بد به علت نفوذ دیگران نیست بلکه به خاطر اشتباهات کاربران می باشد. مطالعات اخیر نشان داده است که ۵۵٪ وقایع امنیتی از سوی کاربران ساده یا غیر ماهر روی می دهد. آنها کاری را که نباید انجام می‌دهند (فولادی، ۱۳۸۱).

امروزه فناوری اطلاعات آنچنان جهان را در سیطره خود قرار داده است که هیچ نقطه ای در امان نیست . خانواده ها دیگر نمی توانند تربیت خاص خود را در مورد فرزندانشان مد نظر قرار دهند. در چنین عرصه ای اگر برای اطلاعات طرح و نقشه جامعی وجود نداشته باشد و بکارگیری آن منطبق با اهداف معین و هوشمندانه نباشد خطرات زیادی جوامع و فرهنگ بشری را تهدید می کند.

نقش اینترنت در امنیت انسانی

دسترسی سریع و آسان به اطلاعات موجب نشر سریع اخبار، رویدادها و ارتقاء آگاهی های عمومی در جامعه می شود. از سوی دیگر امکان یادگیری در هر مکان و زمان و فارغ از محدودیت های فعلی، آموزش همه جانبه برای کلیه اقشار جامعه را فراهم می آورد. لذا

فناوری اطلاعات و ارتباطات و تشکیل جامعه اطلاعاتی می تواند در توسعه فرهنگ جامعه تاثیر بسزایی داشته باشد.

اینترنت به عنوان یکی از مهم ترین محصولات فناوری اطلاعات و سازمانی جهانی است، محیطی است که ارتباط و تعامل میلیونها نفر از کشورها و فرهنگ های مختلف را فراهم می آورد، رسانه ای است که تعامل فرهنگی را در سطحی وسیع میسر می سازد. توانایی ما در اثر گذاری بر این محیط به نسبت تاثیراتی که تاکنون بر تلویزیون یا تلفن داشته ایم بیشتر است، چرا که همزمان می توانیم به عنوان تولید کننده و همچنین مصرف کننده محتوای اطلاعاتی در اینترنت داشته باشیم. اما در مورد رسانه انعطاف ناپذیری مانند تلویزیون، به این شکل مطرح می شود که آیا دستگاه تلویزیون را روشن کنیم یا نه و چه برنامه ای را تماشا کنیم.

اینترنت دنیایی مجازی ایجاد نموده که حتی روابط خانوادگی را نیز تحت تاثیر قرار داده است. با استفاده از دنیای مجازی جدید جهش علمی و ارتباطی بزرگی در حال روی دادن است که فرهنگ و شیوه زندگی مردم را تغییر می دهد.

در گستره روابط انسانی، اینترنت ابزاری به نسبت نو پاست و از دیدگاه روان شناختی با نگاهی موشکافانه به رویدادها، درمی یابیم که این ابزار تا چه اندازه ممکن است بر زندگی ما اثر گذارد. پژوهش هائی که در مورد رفتار واقعی افراد در هنگام ارتباط مستقیم شبکه ای انجام گرفته، نامنسجم و ناچیز است، لیکن این موضوع به سرعت مورد توجه رشته های گوناگون علمی قرار گرفته است (والیس، ۱۳۸۲).

اینترنت زندگی انسان را متحول می کند و بر فرهنگ وی تاثیر گذار است. برای فهم اینکه اینترنت تا چه حد می تواند بر فرهنگ موثر باشد، آنچه که ارائه می کند و می تواند ارائه نماید را شناخت . اینترنت قطعاً با ارائه روش های سریع و کارا در مورد همه وقایع سنن ، آداب و رسوم جهان می گردد، آموزش کلاسیک را متحول کرده و از این طریق دانش عمومی جامعه تغییر نموده و یکی از مولفه های فرهنگ متحول می شود. تحقیقات نشان می دهد که اطلاعات در شبکه اینترنت کاربردهای مختلفی را در بر می‌گیرد از جمله می توان به موارد ذیل اشاره کرد:

اطلاعات تجاری، اطلاعات علمی، اطلاعات پزشکی – بهداشتی، صفحات شخصی، انجمن های علمی، مباحث اجتماعی، اطلاعات دولتی و اطلاعات مذهبی. در این میان حجم اطلاعات تجاری بسیار زیاد و قابل توجه است و معمولاً به هنگام جستجو در اینترنت بیش از هر چیز با اطلاعات تجاری مواجهیم.

خدمات متنوعی که تحت وب می پردازیم و در بستر اینترنت قابل استفاده است، هر یک می تواند بر فرهنگ و امنیت انسانی اثر گذارد:

الف – صفحات شخصی

ویژگی مثبت صفحات شخصی آن است که به ما امکان می دهند اطلاعات شخصی خود را در معرض دید دیگران قرار دهیم، با شمار چشمگیری از افراد دیگر درباره زندگی مان به داد و ستد داده ها بپردازیم و نظرات افرادی را که به وب سایت ما دسترسی دارند، دریافت نماییم. یکی از مشخصه های منفی رشد و گسترش صفحات شخصی آن است که ظاهراً آنها انبوه بسیاری از مطالب بی فایده و بی مایه را وارد اینترنت می نمایند. شاید شبکه، بزرگ ترین و ارزان ترین راه درج مطالب پوچ و بیهوده در گیتی است و دارای کانالهای پخشی است که حتی در گمان ناشران بزرگ نمی گنجد. زمانی که واژه های کلیدی به گونه ای تصادفی انتخاب و در دسترس موتورهای کاوش قرار می گیرد، اغلب ده ها صفحه ی شخصی نا مربوط را نمایش می دهند و هنگامی که در جست و جوی داده هایی هستید، سردرگمی و بی نظمی فراوانی را پدید می آورند.

ب – پست الکترونیکی

تا کنون از پست الکترونیکی (یا به اختصار E-Mail) بیش از سایر خدمات مبتنی بر اینترنت استفاده شده است. در واقع بسیاری از مردم تنها از پست الکترونیکی در اینترنت استفاده می کنند. پست الکترونیکی ارسال پیغام های یک به یک بین اشخاص را ممکن می سازد اما هیچ امکانی برای ارتباط بر خط ارائه نمی کند.

توسط رسانه پست الکترونیکی هر نوع داده ای اعم از صوت، تصویر و غیره به صورت اختصاصی منتقل می شود. پست الکترونیکی به صورتی مخفی تر از پست عادی ارتباط مشروع و نامشروع اشخاص را برقرار می کند. این ارتباط می تواند نامه های محاوره ای بین دو دوست یا دو شخصیت علمی راجع به موضوعی خاص و یا نامه دانشجو به استاد برای رفع مشکلات درسی باشد. علاوه بر آن شرکت های تجاری با جمع آوری آدرس های پست الکترونیکی بالقوه اقدام به تبلیغ پیرامون محصولات و خدمات خود می‌نمایند. از لحاظ فرهنگی این عمل هنگامی خطرناک است که همراه با تبلیغ محصولات ساخت بشر، به ترویج فرهنگ و تحریک طبیعت اشخاص به انواع حیل نیز می پردازند.

ج – گپ زنی و کنفرانس های صوتی و تصویری

در اینترنت ابزارهای مختلفی برای گفتگوی رودررو ایجاد و توسعه داده شده اند. منظور از گفتگوی رودررو هر نوع ارتباطی است که شخص در آن پیامهایی را بصورت بلادرنگ (یعنی ، در حین اینکه منتظر است) با فرد دیگری مبادله می کند. ابتدائی ترین سرویس گپ زنی

اجازه می دهد که از طریق تایپ، پیام هائی با شخص دیگر رد و بدل شود. هر پیامی که در پنجره گفتگو تایپ می شود در پنجره طرف دیگر منعکس شده و بالعکس. این نوع گپ زنی، گپ زنی اختصاصی گفته می شود. بعضی از سیستم های اجازه می دهند که در هر زمان با بیش از یک شخص گفتگو کرد که به عنوان گپ زنی عمومی شناخته می شود. گفتگوهای پیشرفته امکان انتقال صوت را نیز ممکن ساخته اند و دو طرف گفتگو کننده می توانند صدای یکدیگر را بشنوند. نسخه پیشرفته تر آن انتقال تصویر به صورت زنده را ممکن ساخته است که طرفین می توانند همچون ارتباطی نزدیک یکدیگر را دیده و احساسات خود را به صورت قوی منتقل نمایند.

چنانچه هرگز در گفتگوهای اینترنتی شرکت نکرده باشید، این نوع برقراری ارتباط باید خنده دار بنظر آید. گویا ، ارتباط چندانی بین آدم ها برقرار نیست و بیشتر گفته ها، انبوه درهم و برهمی از اهانت های بی وقفه و غرغرکردن های بی معناست. با وجود این، گفتگو کننده های مجرب یاد می گیرند که موضوعات بحث (زنجیره ها) را به گونه ای دنبال نمایند که گویی در اتاقی نشسته اند که همزمان، چندین گفتگو در آن جریان دارد. آن ها ممکن است به طور کامل در یک گفتگو شرکت کنند و بقیه را فقط پنهانی به گوش بایستد. در این گفتگوها، تجزیه و تحلیل موضوعات بحث، به این علت راحت تر است که پیام ها حرکت پیمایشی کندی دارند و برای مدتی بر روی صفحه ی نمایشگر کامپیوتر باقی می مانند. سردرگمی و سوء استفاده های احتمالی در این ارتباطات می تواند جنبه هایی از تهدید امنیتی محسوب گردد.

د – تشکیل گروههای مجازی

درست همان گونه که گروههای واقعی تفاوت های بسیاری دارند، گروههای مجازی نیز انواع گوناگونی دارند. بسیاری از گروههای مجازی بطور عمده متشکل از افرادی هستند که کم و بیش همدیگر را می شناسند و از شبکه تنها برای تماس و درمیان گذاشتن نظرات خود در نشست های رودررو سود می جویند. پیشگامان اصلی شبکه اغلب با این رسانه چنین برخوردی دارند. سایر گروههای مجازی، افرادی با دلبستگی های مشترک را که تاکنون یکدیگر را نمی شناخته اند، از طریق شبکه متحد می سازند. چنانچه شرایط و مقتضیات زمانی اجازه دهد، پاره ای از این افراد ممکن است سرانجام یکدیگر را در گردهمائی ها، جلسات کاری، یا همایش های اجتماعی دیدار نمایند. بنابراین دست دادن با کسی که به مدت طولانی در شبکه با وی در ارتباط بوده اید رویدادی شگرف نیست. در عین حال ممکن است برداشت های شما از تعاملات درون شبکه ای با آن شخص، ناگهان با دیداری رودررو متحول گردد، و دچار شگفت زدگی شوید.

در گروههای کاری، احتمال اینکه همه ی افراد مطالب یکسانی بدانند، بعید است. به عبارت بهتر اعضای گروه پس از طرح موضوع و گفت و شنود درباره ی آن ، از اطلاعات و عقاید سایرین نیز آگاهی می یابند. هر یک از افراد می توانند در دانسته های دیگران سهیم شوند و دانسته های خویش را در اختیار آنان بگذارند و بدین ترتیب انتظار می‌رود کل دانسته ها، دست کم چند برابر مجموع اجزای تشکیل دهنده ی آن شود. متاسفانه اغلب، اوضاع این گونه نیست و به ویژه در مواردی که گروههای کاری برای تصمیم گیری در شبکه گرد هم می آیند، چنین نمی شود. گاه ممکن است گروهها از قطبیت دچار آسیب شوند، زیرا اعضاء در مشارکت دانسته های خویش با دیگران، تقریباً به شکل گزینشی عمل می کنند و احتمال طرح اطلاعاتی که ممکن است بر خلاف هم اندیشی در حال شکل گیری گروه باشد، کمتر می شود در نتیجه، گفتگویی سوگرایانه است که در آن، هیچ امکانی برای بررسی همه ی حقایق وجود ندارد، چرا که اعضا همه ی آن حقایق را عنوان نکرده اند. لطمات شخصیتی و عاطفی در کنار ارائه ی اطلاعات غلط آسیب هایی که در این مراودات ممکن است بروز نماید.

اینترنت و اتلاف وقت

اینترنت ممکن است آنچنان گیرا و آنقدر سرگرم کننده باشد که افراد را به استفاده ی فشرده و حتی مفرط و بی اختیار از آن وادار سازد. در اوایل سالهای دهه ۱۹۹۰، اشاره به این که انسان ممکن است به استفاده از اینترنت معتاد شود، اغلب با خنده ی بلند روبرو می شد ولی با پدیدار شدن علایم بیشتری از این موضوع (خواه به شکل روایت یا از طریق بررسی و افزایش شمار کسانی که برای گریز از این نارضایتی، از متخصصان درخواست کمک می کردند) اعتیاد به اینترنت به صورت واقعیتی درآمده است.

تصور کنید بدون دانستن محل کتابی خاص یا دانستن موضوع مورد مطالعه به کتابخانه بزرگی وارد شده اید. هر کتابی را که بر می دارید سپس به کتاب دیگری مشغول می شوید بدون اینکه خود بدانید وقت خود را تلف نموده اید. در اینترنت نیز موضوع جالب توجه، بسیار است از اخبار ورزشی گرفته تا تبلیغات شرکت ها. اگر ندانید به دنبال چه می گردید و به چه میزان فرصت دارید ، وقت خود را تلف کرده اید. با توجه به این مشکل اساسی است که اکنون سخن از اینترنت دوم و یا اینترنت علمی به میان می آید.

اینترنت و مطالب غیر اخلاقی

یکی از بحث انگیز ترین ویژگی های اینترنت وجود مطالب و تصاویر غیر اخلاقی بویژه برای کودکانی است که به اینترنت دسترسی دارند که معمولاً انگیزه اصلی و زمینه ساز تلاش

برای کنترل و محدود سازی دسترسی به اینترنت است. در سال ۱۹۹۵، سنای آمریکا نمایش تصاویر موهن از طریق شبکه ی کامپیوتری را ممنوع اعلام کرد و برای کسانی که آگاهانه، تصاویر زننده ای را در اختیار کودکان زیر ۱۸ سال قرار می دهند، پرداخت جریمه و محکومیت زندان تعیین نمود. این گونه استفاده نامطلوب از اینترنت به عنوان تهدیدی برای فرهنگ و امنیت جوامع محسوب شده و خطرات بسیاری را بدنبال خواهد داشت. به همین دلیل کشورها سعی می کنند تا به گونه ای به کنترل چگونگی به کارگیری اینترنت بپردازند.

شخصیت انسان و محیط مجازی

ملاک های شخصیتی انسان در محیط مجازی (شبکه ای) با معیارهای مربوط به دنیای فیزیکی چندان تفاوتی ندارد. به عبارت بهتر اگر در دنیای واقعی نوع رفتار یک شخص با سایرین گویای شخصیت او باشد، در دنیای مجازی هم همان ملاک ها وجود دارد اگر چه شکل صوری آن تفاوت می کند. یعنی نوع رفتار و تعاملات انسانها با یکدیگر در محیط شبکه ای یا مجازی (به عبارت دیگر اخلاق الکترونیکی) مبین شخصیت آنان است. به عنوان مثال رفتار مشتری در قبال فروشنده در سیستم تجارت الکترونیکی، رفتار دانشجو در برابر استاد در محیط آموزش الکترونیکی و عملکرد کارگر در قبال کارفرما در بستر دور کاری نمونه هایی از تعاملات تحت وب محسوب می شوند.

ویژگی ها و صفات انسانی همچون صداقت، قانونمندی، احترام به تعهدات، همکاری گروهی و سایر موارد مشابه در یک محیط مبتنی بر وب نیز معنا می یابد. صداقت به معنی درستی و راستی در گفتار و کردار، در یک محیط شبکه ای به معنی دوری از نیرنگ و فریب کاری است. قانون مندی به معنی تبعیت از قوانین وضع شده برای محیط وب، همانند پیروی از قوانین مالکیت معنوی و عدم سوء استفاده از اطلاعات در محیط شبکه است. احترام به تعهدات به معنی وفای به عهد در محیط وب می باشد. به عنوان مثال دانشجو بر اساس تعهدات خود در محیط آموزش الکترونیکی تکالیف خود را انجام دهد. همکاری گروهی و عدم انزوا جویی، به معنی میزان مشارکت در فعالیت های گروهی تحت وب در زمینه های مختلف می باشد. نوع و چگونگی استفاده از وب نیز یکی دیگر از معیارهای معرف شخصیت کاربر است. اینکه کاربر بیشتر به دنبال استفاده از گپ زنی باشد، یا در پی خرید و تجارت، از تعاملات علمی مبتنی بر وب بهره جوید ، یا به دنبال مزاحمت باشد، گویای شخصیت اوست.

تثبیت هویت ملی در اینترنت

تثبیت هویت هر ملت در محیط اینترنت مستلزم اعمال سیاست هایی به منظور افزایش ضریب نفوذ اینترنت در آن کشور است. استفاده از اینترنت در کاربردهای روزمره زندگی حضور هر چه بیشتر شهروندان جامعه را بدنبال دارد. روش های ذیل موجب تقویت نقش یک جامعه در محیط مجازی خواهد بود :

- ✓ افراد جامعه از آدرس های پست الکترونیکی برخوردار باشند و مکاتبات خود را از آن طریق انجام دهند.
- ✓ شهروندان و علی الخصوص خبرگان و زبدگان (شبیه دانشگاهیان ، صنعتگران) جامعه از سایت وب شخصی برخوردار باشند و از آن طریق به معرفی سوابق، فعالیت ها و توانائی های خود بپردازند.

بدیهی است که این روش ها نیز به نوبه ی خود در معرض تهدید و آسیب قرار دارد.

امنیت انسانی و فناوری اطلاعات و ارتباطات

امنیت انسانی چیزی بیش از نبود ستیز و مشاجره است. امنیت با تعلیم و تربیت و سلامتی، دموکراسی و حقوق انسانی، محافظت در برابر بلایای طبیعی و کاهش سلاح های کشنده همراه است. امنیت همچنین ممکن است اشاره کند به مفهوم آزادی برای خواستن و شامل امنیت اقتصادی، غذایی، سلامتی، محیطی، سیاسی، و اجتماعی است. عدم امنیت انسانی همزاد شده است با صنعت جهانی سازی لیبرال نو، نظامی سازی، ترافیک، سکس، نابرابری اجتماعی، فقر، تروریسم و مشاجرات قومی، که چالش بزرگ در ابتدای قرن ۲۱، هم در کشورهای پیشرفته و هم در کشورهای در حال رشد است. (سومناروگا[1] ۲۰۰۴).

عدم امنیت توسعه ی انسانی[2] را به مخاطره می اندازد. توسعه ی انسانی به عنوان فرایند گسترش انتخاب های مردم تعریف شده است. بیشترین این انتخاب ها، توانایی برای زندگی طولانی و سالم، دسترسی به تعلیم و تربیت و دسترسی به منابع مورد نیاز برای تأمین زندگی استاندارد است (پتروفسکی[3] ۲۰۰۵).

در نگاهی کلی، تلاش برای مقابله با تمامی آنچه که بقا، زندگی روزمره و شأن انسان بودن را تهدید می کند در زمره ی امنیت انسانی قرار می گیرد. در این دیدگاه اعتقاد بر آن است که انسان می بایست قادر باشد بدور از هرگونه تهدیدی زندگی خود را هدایت

---

[1] Somnaruga, Carnelio
[2] Human Development
[3] Petrovsky, Vladimir

کند. بنابر این «امنیت انسانی» می تواند به عنوان حفاظت و صیانت از بقاء انسان و زندگی روزمره (که می توان آن را در مقابل مرگ زودرس، بیماری های قابل اجتناب، و مشکل بزرگ بی سوادی فرض کرد) و همچنین اجتناب از هتک حرمت که می تواند زخم بزرگی بر پیکره ی زندگی ما باشد (مانند فقر، تنگدستی، حبس، محرومیت و ...) تلقی شود سن[1] (۲۰۰۲) با تأکید بر این معنی، معتقد است مفهوم «امنیت انسانی» حداقل می بایست شامل عوامل زیر بشود:

۱. تمرکز روشن روی زندگی فردی انسان (که ممکن است با فکر تکنوکرات امنیت اجتماعی یا تفسیر امنیت در زمینه ی نظامی در تضاد قرار گیرد).
۲. قدرشناسی نسبت به نقش جامعه و آرایش اجتماعی در هر چه امن تر ساختن زندگی در یک مسیر سازنده. (پرهیز از جدایی جامعه از وضعیت خطرناک و یا رستگاری فرد که در زمینه های مذهبی مورد تأکید قرار می‌گیرد).
۳. تمرکزی معقول روی خطرات پیش روی انسانی.
۴. تمرکزی انتخاب شده برای تأکید بیشتر بر حقوق اولیه انسان.

فناوری اطلاعات و ارتباطات، به عنوان یکی از مهم ترین دستاوردهای بشری که به سرعت در حال گسترش است، می تواند هم به عنوان فرصت و هم تهدید امنیت انسانی مطرح باشد. برخی از فرصت هایی که توسعه ی فاوا[2] ایجاد کرده است عبارتند از:

- فراهم سازی بستر مناسبی برای تبادل و گسترش دانش با بهره گیری از امکانات ارتباطی، پایگاه های اطلاعاتی و توانمندی ایجاد شده برای ذخیره، پردازش و بازیابی اطلاعات.
- تسهیل تبادلات و ارتباطات فرهنگی- اجتماعی در سطح جهانی با بهره گیری از شبکه ی جهانی اینترنت
- ارتقاء سطح آگاهی های عمومی جامعه نسبت به مسائل اجتماعی، سیاسی، فرهنگی، بهداشتی، اقتصادی و حقوق اولیه ی انسان ها
- کمک به رونق اقتصادی با بهره گیری از امکاناتی چون تجارت الکترونیکی، تبلیغات و ...
- فراهم سازی امکان رشد شخصی از طریق بهره گیری از انواع آموزش های الکترونیکی و کمک به ارتقاء کیفیت فعالیت های آموزشی با بهره گیری از فاوا

در مقابل، توسعه ی سریع فاوا، تهدیداتی را نیز به دنبال داشته است:

---

[1] Sen, Amartya
[2] Information and Communication Technology (ICT)

- شکاف دیجیتالی بین کشورهای فقیر و غنی که متأسفانه با رشد حیرت انگیز این فناوری ها به سرعت رو به گسترش است.
- تهدید حریم خصوصی افراد با بهره گیری از فاوا حتی توسط دولت ها در پاره ای از موارد
- سوء استفاده ابزاری از این فناوری ها توسط تبه کاران در جهت گسترش جرم و جنایت و فحشا
- سوء استفاده از پیشرفت های تکنولوژیک در صنایع نظامی و گسترش تهدیدهای نظامی

سخن پایانی

فناوری اطلاعات و ارتباطات در زندگی انسان ها بطور همه جانبه رسوخ کرده است. اکنون دیگر نمی توان به این فناوری های صرفاً به منزله ی ابزارهایی نگریست که در پاره ای موارد مورد استفاده قرار می گیرد، بلکه ورود فاوا با تغییر رویکرد در بسیاری از مسائل مبتلابه جامعه ی انسانی همراه بوده است. دولت، تجارت، تعلیم و تربیت، مدیریت و فرهنگ با تحولاتی اساسی تحت تأثیر فاوا روبرو شده است.

در این میان امنیت انسانی نیز از آنجا که عوامل تهدید کننده ی آن دچار تحول و دگرگونی شده است، معنایی تازه می‌یابد. از این روست که «امنیت انسانی» امروزه مستلزم مدیریت جدید است. در این نظام مدیریتی جدید می بایست اصولی مورد توجه قرار گیرد:

- اکنون با چالش های جهانی در مقوله ی امنیت انسانی روبرو هستیم، و لذا نیازمند پاسخ های جهانی و نظامی بین المللی برای مقابله خواهیم بود. ضرورت وجود یک سیاست جهانی «امنیت انسانی» که بر روی مسؤولیت همه تأکید دارد غیر قابل انکار است. مشکلی جهانی، نیازمند عزمی جهانی برای مقابله است.
- نظریه ی تأخیر فرهنگی اعتقاد دارد که گسترش فناوری ها همواره سریع تر از گسترش فرهنگی بوده است. این واقعیتی است که در مقوله ی فناوری اطلاعات و ارتباطات نیز صدق می کند. این فناوری ها با سرعت حیرت آوری گسترش یافته اند، در حالی که معضلات فرهنگی چگونگی بهره گیری از آنها همچنان باقی است. از این رو توجه به جنبه های انسانی در کنار جنبه های فنی امنیت، ضرورت می یابد و بر متولیان فرهنگی است که در راستای شکل دادن به فرهنگ

مناسب بهره گیری از فناوری و توسعه و ترویج آن به سختی بکوشند. در این میان توجه به تعالیم راستین مذهبی بسیار چاره ساز خواهد بود.

- امروزه فناوری اطلاعات و ارتباطات به عنوان عامل تهدید کننده ی امنیت انسانی مطرح است، پس ضروری است که این فناوری ها در مقابله با این تهدید ها نیز ایفای نقش نمایند. بهره گیری از قدرت زاید الوصف فناوری های نوین در مقابله با آنچه امنیت انسانی را تهدید می کند به عنوان یک ضرورت غیر قابل انکار پیش روی ما قرار دارد و می بایست با گسترش آگاهی ها و سواد لازم، راه های سوء استفاده از آن مسدود شود تا دستیابی به امنیت ممکن گردد. در جایی که والدین توانایی بهره گیری از رایانه و اینترنت را ندارند، بطور طبیعی این احتمال بروز پیدا می کند که فرزندان در بهره گیری از آنها به خطا روند، چرا که هیچ کنترلی بر خود احساس نمی کنند و میدان برای سوء استفاده کنندگان باز می ماند. مادام که والدین توانایی و اطلاعات کافی در هدایت و کنترل فرزندان را در این زمینه نداشته باشند، با نوعی تهدید امنیت روبرو خواهیم بود. این مثالی روشن از ضرورت تجیز به فناوری برای مقابله با تهدیدهای جدید امنیتی است.
- با توجه به انواع مخاطرات موجود، طراحی هر سیستم فناورانه می بایست با اندیشه و طراحی در مورد سیستم مدیریت امنیت آن همراه باشد. سیستمی که با قوانین مورد توافق جهانی در این زمینه هماهنگی داشته باشد و قادر باشد در حداکثر ممکن به مقابله با تهدیدات باشد. همچنان که برنامه ریزی فرهنگی (طبق آنچه قبلاً ذکر شد) به طور همزمان ضرورت می یابد.

منابع

۱- سلماسی زاده، محمود. (۱۳۸۰). جنگ اطلاعات و امنیت. مجموعه مقالات اولیشن کنفرانس رمز ایران.

۲- فتحیان، محمد.، مهدوی نور، سید حاتم. (۱۳۸۶). مبانی و مدیریت فناوری اطلاعات. تهران: انتشارات دانشگاه علم و صنعت ایران. چاپ دوم.

۳- فولادی، قاسم.، صفات، جواد. (۱۳۸۱). جنگ اطلاعات به سبک چینی. تهران: موسسه آموزش و تحقیقات صنایع دفاع.

۴- ملکیان، احسان. (۱۳۸۱). نفوذگری در شبکه و روش های مقابله. تهران: موسسه علمی فرهنگی نص.

۵- والیس، پاتریکا. (۱۳۸۲). روانشناسی اینترنت. ترجمه بهنام اوحدی. تهران: انتشارات نقش خورشید.

6- CSPP. (2005). Retrieved from: http//www.cspp.org 2005

7- Mann, Edward. (1993). USAF,one target, one Bom is the principle of mass dead? military review. September.

8- Pertovsky,Vladimir. (2005). Human development and Human security in EURASIA. International Journal on world peace. Vol. XXII No. 4 December.

9- Sen, Amartya. (2002). Basic Educatio and Human Security. In Commission on Human Security, Retrieved November 2008 from: http://www.humansecurity-chs.org/activities/outreach/0102Sen.html

10- Sommaruga, Cornelio. (2004). The global challenge of human security. The Journal of Futures Studies, Srategic Thinking and Policy, 6, 4; Academic Tesearch Library. Pg. 208.