تبیین تهدیدات سیستم های اطلاعات از منظر کاربران

علی ربیعی
دانشیار و عضو هیئت علمی دانشگاه پیام نور، alirabiee@csr.ir

هاجر آصف
کارشناسی ارشد مدیریت بازرگانی بین الملل دانشگاه پیام نور، assef.hajar@gmail.com

چکیده:

این مقاله بر اساس تحقیقی با مفروض احساس تهدید و نا امنی سامان یافته است و در پی پاسخ به این پرسش است که تهدید ادراک شده توسط شهروندان چگونه است. احساس تهدید و ناامنی از سوی شهروندان، پدیده‌ای است که دارای تبعات روانی و اجتماعی است و نیاز به یک تحقیق و سنجش برای درک این نوع تهدیدات وجود دارد. این پژوهش به مطالعه تهدیدات مهم سیستم‌های اطلاعاتی و همچنین تحلیل بالاترین تهدید احساس شده از سوی شهروندان تهرانی می‌پردازد.

این تحقیق از جنبه هدف، توسعه‌ای و تا حدودی کاربردی است. از نظر ماهیت، تحقیقی توصیفی پیمایشی است. در مرحله اول برای به‌دست آوردن تهدیدات مهم از سوی سیستم‌های اطلاعاتی، به روش هدف‌دار، تعداد ۱۰ نفر از متخصصین دانشگاهی انتخاب و به روش دلفی، مهم‌ترین تهدیدات استخراج شده‌اند. این تهدیدات در قالب پرسشنامه و با حجم نمونه ۳۳۰ نفر از میان شهروندان تهرانی که به نوعی در معرض سیستم‌های اطلاعاتی قرار گرفته‌اند، پیمایش شده‌اند. یافته‌های تحقیق حاکی از آن است که از بین تهدیدات فردی، اخلاقی، سیاسی ـ روانی، اجتماعی ـ اقتصادی و فرهنگی، بالاترین تهدید احساس شده، تهدیدات سیاسی ـ روانی هستند.

کلید واژه‌ها : سیستم‌های اطلاعات، تهدیدات فردی، تهدیدات اخلاقی، تهدیدات سیاسی ـ روانی، تهدیدات اجتماعی ـ اقتصادی، تهدیدات فرهنگی .

مقدمه :

در این مقاله می‌کوشیم تا به تشریح امنیت فردی در مواجهه با سیستم‌های اطلاعاتی بپردازیم. در حقیقت شناخت و تهیه فهرستی از معایب و تهدیدات این سیستم، پایه‌ای برای تعریف نیازهای امنیتی هستند. زمانیکه تهدیدات و مسائل احتمالی شناخته شدند، قوانینی را می‌توان به منظور کنترل عملیات شبکه و رفع مسائل تدوین کرد .

در این مقاله تقریبا همه تهدیدات سیستم-های اطلاعاتی طبقه بندی شده‌اند و آثار این پدیده که منجر به آشفتگی و به هم ریختگی حوزه‌های فردی، فرهنگی، اخلاقی، سیاسی و مواردی از این قبیل شده، در قالب یک مدل نشان داده شده‌اند.

در طول دو دهه اخیر، مدیران شاهد یک دوره تغییر شگرف جهانی به‌واسطه پیشرفت فنآو ری، جهانی شدن بازارها و تبادل اطلاعات بوده‌اند. تحولات عظیمی که در جهان رخ داده، زمینه پیدایش اقتصاد جهانی، کسب و کار جهانی و حرکت از جامعه صنعتی به سمت عصر اطلاعات محوری را فراهم کرده است. در این محیط متغیر، نوآوری در محصولات و فرآیندهای سازمانی،

به‌مثابه عاملی حساس و حیاتی در موفقیت شرکت‌ها مطرح می‌شود. یکی از این زمینه‌های نوآوری، کسب اطلاعات جدید و اتخاذ فنآوری اطلاعات است.

در جوامع امروزی در بیشتر بخش‌های کسب و کار، از فنآوری اطلاعات استفاده می‌شود و می‌توان گفت این فنآوری بخشی از زندگی روزانه و شخصی افراد شده است. در واقع سیستم‌های اطلاعاتی کارا و یکپارچه که بتوانند همه فعالیت‌ها و وظایف یک سازمان را پوشش دهند، از ابزارهای مفیدی هستند که سازمان‌ها و افراد برای افزایش قابلیت‌های خود، بهبود عملکرد، تصمیم‌گیری بهتر و دستیابی به مزیت رقابتی از آنها استفاده می‌کنند. در واقع در این عصر اطلاعات، دو منبع قدرت یعنی کامپیوترها و ارتباطات، تغییرات فنآوری و پیشرفت‌ها را دامن می-زنند.

این پیشرفت‌ها در عرصه اطلاعاتی، امکان دسترسی سریع و آسان را به منابع به اشتراک گذاشته شده سازمان‌ها و شرکت‌ها پدید آورده است و همانند هر پدیده جدید دیگر، با وجود همه منافع و فرصت‌هایی که برای تسریع ارتباطات انسانی دارند، تهدیدات زیادی نیز برای مردم و دولت‌ها به همراه می‌آورند (برن استین[1]، 2006).

در چنین فضای اطلاعاتی‌ای، ما همواره در معرض تهدیدات الکترونیکی از قبیل جرایم سازمان یافته، تخریب بانک‌های اطلاعاتی، نقض حقوق مالکیت معنوی و اطلاع رسانی‌های غلط و آسیب پذیر شدن فضای تبادل اطلاعات هستیم (منس[2]، 2007).

با این تفاسیر، سیستم‌های اطلاعاتی در محیط پر از خطر پیاده می‌شوند. این خطرات دامنه وسیعی دارند. از دله دزدی گرفته تا سرقت‌های بزرگ، از کلاهبرداری کم تا سهل انگاری‌های عمده، از سوء تفاهمی مختصر تا سر در گمی کامل، از یک خطای کوچک تا عدم صلاحیت فاحش، از ناشی گری‌های بی‌ضرر تا خرابکاری، از گوش دادن بدون قصد تا استراق سمع فعال. باید به این نکته توجه داشت که در آینده فنآوری اطلاعات بیشتر از امروز پیشرفت می‌کند و از این رو به تلاش بیشتری برای شناسایی و رفع تهدیدات آن نیازمندیم. این مقاله کوششی در راستای شناسایی این تهدایدات است.

تهدیدات ناشی از سیستم های اطلاعات :

۱- تهدیدات فردی:

۱-۱ ردیابی از طریق وب

فایل‌های ثبت، مهم‌ترین منبع برای یافتن اطلاعاتی درباره چگونگی استفاده کاربران از سایت هستند. تحلیل فایل‌های ثبت هم به معنای ارایه داده‌ها به یک ارایه دهنده خدمات نرم‌افزاری است و هم به مفهوم نصب نرم‌افزاری است که بتواند اطلاعات مربوطه را از فایل‌های موجود در سازمان انتخاب کند. با استفاده از نرم‌افزار رد یابی، شرکت‌ها می‌توانند حرکات اشخاص در

[1] Bernstein
[2] Mannes

اینترنت را دنبال کنند. کوکی ها[3] از جمله این نرم افزار ها هستند که دغدغه‌های مربوط به حریم خصوصی را بر انگیخته اند (توربان و دیگران ،۱۳۸۶: ۳۱۳).
به عنوان مثال "گوگل ارث"[4] برای تمامی کاربران اینترنت در سراسر دنیا نامی آشناست. این نرم‌افزار حاوی یک کارت گرافیک نسبتا قوی است و با یک اتصال ساده به اینترنت می‌تواند تصاویر نیمه زنده‌ای را که توسط یک ماهواره عکس‌برداری تخصصی به زمین مخابره می‌شود، ببیند و حتی خانه و محل کارشان را روی نقشه‌هایی که با دقت‌های عظیم زوم می‌شوند، بیابند. بسیاری از کارشناسان رسانه‌ای و حتی سران سیاسی بلند پایه، این نرم افزار را یک نرم‌افزار جاسوسی می‌دانند که قوانین بین‌المللی و امنیت ملی کشور ها را نقض می‌کند و تهدیدی بر صلح جهانی است (کراوت[5]، 2009).
مثال دیگری که می‌توان از نرم‌افزار های ردیاب برای ردیابی در وب استفاده کرد جی‌پی‌اس است. این نرم‌افزار برای کنترل اشخاص یا خودرو در حین خطر طراحی شده است اما امروزه مصارف دیگری نیز دارد. باید اذعان داشت که حتی با غیر فعال کردن برخی ویژگی‌های مرورگر های اینترنتی، روش‌های متعددی برای شناسایی افراد در فضای وب وجود دارد (سازمان پدافند غیر عامل کشور،۱۳۸۹).

۱-۲ دسترسی به اطلاعات شخصی و استراق سمع

گوش فرا دادن به محاورات و گفتگوهای بین افراد با استفاده از وسایل و تجهیزات ارتباطی الکترونیکی منجر به پایمال شدن بدیهی‌ترین حقوق شهروندی شده است که در آن ناشناخته بودن و در خلوت خود بودن امری کمیاب است.
به‌طور کل سازمان‌های بزرگ عمومی و خصوصی مثل دولت، که همواره در صددند بر روابط بین افراد و سازمان‌ها حکومت کنند، هیچ وقت از جریان اطلاعات بین افراد غافل نمی‌شوند و در این بین گروه‌های کوچک‌تر مثل پلیس، به جمع‌آوری اطلاعات برای سازمان‌های بزرگ می‌پردازند (صرافی نژاد و علی پناهی، ۱۳۸۰: ۳۳۶).
برای نمونه، شنود تلفن از همان آغازین روزهای رواج این فنآوری، به صورت تفنّنی توسط اپراتورهای مراکز تلفن انجام می‌گرفت اما به مرور زمان ورود سرویس‌های جاسوسی و گروه‌های تروریستی و اخلال‌گران، به این حوزه نیز رخ داد (اسدی، ۱۳۸۴: ۳۵).

۱-۳ نقض آزادی‌های فردی و حقوق مدنی

مطالعه تاریخ جوامع نشان‌دهنده تلاش بشر برای دست‌یابی به آزادی و فقط آن است. به تعبیری حق آزادی از سوی خالق به انسان عطا شده است و در دوران اخیر با تلاش‌های علمی انسان‌ها شرایطی پیش آمده است که فنآوری های بشرساخته بی‌درنگ وی را به بند می‌کشند. انسان که

[3] cookie
[4] Google Earth
[5] Kravets

در طول تاریخ برای آزادی مشقت‌های زیادی کشیده، حالا خود شاهد به سخره گرفتن مرموزانه بسیاری از حقوق طبیعی خویش است. حمله به مسائل خصوصی افراد به دو روش انجام می‌شود. آسیب رساندن به اطلاعات شخصی و تجاوز به اطلاعات خصوصی (فانک[۶]،2005).

۱-۴ گسترش تجسّس اطلاعات

در گذشته نظارت افراد با محدودیت‌ها و استفاده از فنون و تجهیزات تجسّس خاصی میسر بود و تنها توسط بخشی از شخصیت‌ها و مقامات برجسته مانند رهبران مذهبی، کارگزاران حکومتی، مراکز وابسته سیاسی و فرهنگی و برخی از اندیشمندان و نخبگان سیاسی و اجتماعی اعمال می‌شد. اما امروزه این مساله تهدیدی برای آحاد جامعه است. گرچه به نظر می‌رسد بعضی از افراد شاغل در برخی حرف بیشتر مورد تهدیدند. از طرف دیگر، تجسّس اطلاعات از سوی دولت‌ها با هدف صیانت از کیان ملی از مواردی است که با گسترش سیستم‌های اطلاعاتی، آسان‌تر شده است. در واقع این سیستم‌های امنیت اطلاعاتی داخلی، خود نوعی تهدید بزرگ به نظر می‌رسند (سوبورنا و سیف الدین خان[۷]،2009).

این امر منجر به بروز رفتارهای خاص به‌صورت ترس، اجبار در پذیرش و مواردی از این قبیل می‌شود (راتمن[۸]،2005).

۱-۵ اضطراب اطلاعاتی

اضطراب اطلاعاتی به دنبال انباشتگی اطلاعات شکل می‌گیرد. در واقع حجم اطلاعات موجود، بسیار فراتر از مقدار زمان لازم برای جذب آن است (استیسی و برایان، ۱۳۸۶: ۵۵).

این ناآرامی می‌تواند به اشکال مختلف مانند کلافگی ناشی از ناتوانی در بر آمدن از عهده حجم داده‌هایی که به زندگی وارد می‌شوند، باشد. اضطراب اطلاعاتی می‌تواند اشکال دیگری نیز به خود بگیرد. شکل دوم این اضطراب، حس ناکامی حاصل از کیفیت اطلاعات موجود روی وب است که بسیار پیش می‌آید که به‌روز یا کامل نباشند. این مورد شامل حس سرخوردگی حاصل از احساس گناه به‌واسطه با خبر نبودن یا دیر با خبردار شدن است (توربان و دیگران ،۱۳۸۶: ۵۵).

۱-۶ هجوم به حریم خصوصی

حریم خصوصی محدوده‌ای است که هر فرد فقط با اراده خود به افشای اطلاعات شخصی‌اش می‌پردازد. منظور از زندگی خصوصی یا خلوت شخصی افراد این است که آنها حق دارند از نظارت و مراقبت و یا دخالت افراد و سازمان‌های دیگر از جمله دولت در زندگی خصوصی خود در امان باشند (صرافی نژاد و علی پناهی، ۱۳۸۰: ۳۳۵).

---

[6] Funk
[7] Suborna & saifuddin khan
[8] Rothman

در راستای پیشرفت انقلاب اطلاعاتی هر چه بیشتر به حریم خصوصی افراد حمله می-شود (فانک،2005). یک مساله حریم خصوصی که به کارکنان نیز مربوط می‌شود، مساله ردیابی است. شرکت‌های زیادی پیام‌های الکترونیکی کارمندان را کنترل می‌کنند و برای این منظور نرم‌افزاری را نصب کرده-اند که فعالیت-های اینترنتی درون سازمان را کنترل می‌کنند تا کارکنانی که زمان زیادی از وقت کاری را صرف امور غیرکاری می‌کنند (سرقت زمان)، مشخص شوند. اما بسیاری از کارکنان نمی‌خواهند که حس کنند حتی در هنگام کار تحت نظر"آقا بالاسر"هستند (توربان و دیگران، ۱۳۸۶: ۳۱۳).

به این دلیل نامه الکترونیکی‌ای که در محیط کاری خود دریافت می‌کنیم، به نوعی می‌تواند سرمایه کارفرما محسوب شود (کریمی، ۱۳۸۲: ۱۹). این امر در نهایت منجر به شیوع استرس در محیط کاری می‌شود. مطالعات نشان می‌دهد که ۵۹٪ از کاربران آی‌تی، هنگامی‌که پشت کامپیوتر خود می‌نشینند، عصبانی می‌شوند (استیسی و برایان، ۱۳۸۶: ۳۸۱).

۱-۷ گسترش سیطره الکترونیکی

اگر چه بهره‌مندی از تجهیزات الکترونیکی حیات بشر را سخت متاثر کرده، و افق‌های نوینی پیش روی وی گشوده است، اما به‌شدت تمام زندگی‌اش تحت تاثیر اطلاعاتی است که صحت و سقم آنها مورد تردید است. این سیطره الکترونیکی واقعیتی است که گاهی زیرکانه بودن اطلاعاتی خاص در جهت القای یک جهان‌بینی مشخص و از پیش تعیین شده و ایجاد شبهه و رسوخ اطلاعات مغرضانه به ذهن گیرنده را تایید می‌کند. به نوعی این سیستم‌های اطلاعاتی در راستای معرفی نسل‌های جدیدی از تجهیزات و در دسترس قرار دادن اطلاعات نوین، به یک تجسس الکترونیکی چند جانبه دست می‌زنند.

فنآوری اطلاعات به دولت‌ها اجازه می‌دهد به‌جای این که در خانه ما را بزنند و از ما بپرسند، به آسانی از برج مراقبت خود، ما را نظاره و کنترل کنند (زاهدی، ۱۳۸۵ :۱۳).

۱-۸ تخریب شخصیت انسان

اگر چه از سویی جریان آزاد اطلاعات می‌تواند به رشد توسعه و بالندگی جامعه و نیز به تکامل انسان منجر شود، اما از سویی دیگر می‌تواند موجبات تخریب شخصیت انسان را نیز فراهم کند و به تبع آن به فروپاشی جامعه انسانی نیز بیانجامد. لذا اندیشمندان علوم اجتماعی و مخصوصاً حقوق‌دانان تمایل دارند تا با استفاده از ابزارهای مختلف، ضمن حفظ دستاوردهای این پدیده نوین از بروز مفاسد بشری جلوگیری کنند (فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی، ۱۳۸۲ : ۴۸).

می‌توان اذعان داشت که به همان سرعتی که رایانه‌ها به عنصر اصلی زندگی تبدیل می‌شوند، منبعی برای گسترش فعالیت‌های خلافکاران و گسترش و شیوع خطراتی هم هستند که نسل

کودک و نوجوان را تهدید می‌کند و به تخریب فضای فکری و شخصیتی کودکان و نوجوانان از راه دستیابی به همه جور سایت، منجر می‌شوند (احمدیان راد، ۱۳۸۷ : ۹).
این موضوع یک مبحث جدی برای والدین به‌وجود می‌آورد. این‌که فرزندانشان تصاویر مستهجن را دریافت کنند یا با جانیانی مواجه شوند که بخواهند آنها را رو در رو ملاقات کنند (استیسی و برایان، ۱۳۸۶: ۳۳۳).

۹-۱ تنش کاری و ایجاد مقاومت در کارکنان

سازمان ها به کارکنان خود اجازه می دهند که به اطلاعات مورد نیاز خود دسترسی داشته باشند.(وود و چفری[9]،2005).از طرفی افزایش در حجم اطلاعات و به نسبت آن کار یا مسئولیت می تواند موجب تنش کاری شود.اگرچه کامپیوتری شدن در افزایش بهره وری در سازمان سود رسانده، اما برای برخی از کارکنان حجم زیادی از کار ایجاد نموده است. بعضی ازکارکنان بویژه آن هایی که خبرگی کار با کامپیوتر را ندارند، ولی مجبورند از آن استفاده کنند، احساس استیصال می کنند و این می تواند بر بهره وری آن ها تأثیر منفی داشته باشد.درصد این استیصال به سواد استفاده از رایانه و اطلاعات باز می گردد.(رضاییان،۱۳۸۱ :۹)
مقاومت کارکنان نیز در برابر تغییر به دلایل مختلفی مثل عامل های شخصیتی ،سهولت کاربری، انتظارات پیشین، وسعت تغییر، احساس نابرابری و مواردی از این قبیل ایجاد می شود.(چهار سوقی ،۱۳۸۶: ۲۰)

۲- تهدیدات روانی سیاسی

۲-۱ جنگ اینترنتی (تروریسم اینترنتی)

تروریسم اینترنتی از حملات اینترنتی است که زیر ساخت‌های اطلاعات ملی در یک کشور را به مخاطره می‌اندازد. در هر کشوری نا امنی‌های داخلی و موارد مشابه آن، می‌تواند باعث کاهش کارآمدی سیستم‌های کامپیوتری و ارتباطی شود و زیر ساخت‌های ملی این کشورها به‌راحتی مورد حمله قرار گیرد. از کار افتادن هریک از شبکه‌های متعدد لن[10] و ون[11] حتی برای مدت زمانی کم، منجر به اشکال‌های بزرگی در پایانه‌های شرکت‌ها و ادارات می‌شود (استیسی و برایان، ۱۳۸۵ : ۳۶۹).
در این میان، بحث اصلی منتقدان سیاسی نرم‌افزار گوگل ارث[12] ـ نرم‌افزار جنجالی ثروتمندترین کمپانی اطلاعات دنیا - این است که تصاویر ارائه شده از تاسیسات نظامی و مخفی کشورها، می-تواند به ابزاری برای حملات تروریستی تبدیل شود (اعتماد ملی، ش ۳۰۸ :۹).

[9] Wood & Chaffery
[10] Local Area Network
[11] Wide Area Network
[12] Google earth

سیستم‌های هدف برای این حملات می‌توانند از سویی شامل سیستم‌های اطلاعات کسب و کار، صنعت و خدمات دولت و رسانه‌ها بوده و از سوی دیگر شامل سیستم‌های فرماندهی نظامی یک کشور باشند (توربان و دیگران، ۱۳۸۶ :۱۱۵۶).

۲-۲ جنگ روانی(شایعه پراکنی)

جنگ روانی، با استفاده از اطلاعات و فنآوری‌های اطلاعاتی نوین توسط کشورهای برخوردار، جهت تثبیت موقعیت ممتاز خود و به‌سان حربه‌ای برای جنگ با سایر ملل و نیل به مقاصد و اهداف سیاسی انجام می‌شود. جنگ روانی در سطح سازمان‌ها با شایعه‌پراکنی انجام می‌شود. مدیران ارشد روی مسایل و موقعیت‌های انفرادی خود تمرکز دارند و به دنبال مقاصد و اهداف خود دست به هر ترفندی می‌زنند (راتمن، 2005).

۲-۳ جنگ مافیایی

اینترنت امکان مناسبی برای تبادل اطلاعات و فعالیت باندهای مافیایی، قاچاق و مواردی از این قبیل است. پول‌شویی به‌واسطه معاملات اینترنتی از رایج‌ترین فعالیت شبکه‌های مافیایی است. ایجاد شرکت‌های مجازی و خرید و فروش‌های غیرقانونی کالاها مثل قاچاق سلاح منجر به پیدایش پول کثیف شده و ایجاد سهام در معاملات بین‌المللی از جمله فعالیت‌های مافیایی اینترنتی است (ربیعی، تقریرات درسی دکتر ربیعی در درس مدیریت بحران‌های ارتباطی، دانشکده علوم اجتماعی دانشگاه تهران، ۱۳۸۸).

۲-۴ تضعیف مبانی دموکراسی در مدیریت دولتی (گسترش سطوح کنترلی بالا دست‌ها)

ماهیت فنآوری اطلاعاتی بیش از آن‌که جهت‌گیری دموکراتیک داشته باشد،گرایش‌های فنآوریک دارد. برای نمونه در کشور سوئیس که دموکراسی مستقیم بر آن حاکم است، مکانیزم‌ها و نهاد-های خاصی که برای این نوع دموکراسی ایجاد شده‌اند، از دخالت و کنجکاوی‌های اینترنت گله-مندند و در مقابل این دخالت‌ها مقاومت می‌کنند. این امر منجر به شکاف قدرت بین دولت و فرد در نظام‌های غیر مردم سالار می‌شود. چون اطلاعات منبع قدرت است و انحصار قدرت به هر نوعی که باشد در بلند مدت تبعات منفی خود را نمایان می‌کند و به جامعه زیان می‌رساند، دولت‌ها به مدد این انحصارطلبی ارزش‌های دموکراتیک را زیر سوال می‌برند (زاهدی، ۱۳۸۵ :۱۱).

۲-۵ تقویت ارزش‌های دموکراتیک (تکثرگرایی، آزادی بیان، آزادی قلم)

با گسترش سیستم‌های اطلاعاتی، مردم از مفاد قانونی مطلع شده، اطلاعات خویش را از راه اینترنت پخش می‌کنند. این امر به‌سان تهدیدی برای برخی از دولت‌ها و فرصتی برای جوامع مدنی است. بر همین اساس در کشور هلند بر خلاف سوئیس، استفاده گسترده از اینترنت باعث

شده است که مردم بتوانند از مفاد قوانینی مطلع شوند که اتحادیه اروپایی انتشار آنها را ممنوع اعلام کرده بود (مستأجران، ۱۳۷۸ :۱۱).

۳- تهدیدات فرهنگی

۳-۱ تهدیدات فرهنگی یک جامعه (به لحاظ اخلاقی ،عقیدتی،اجتماعی)

اطلاعات و شاهراه‌های ارتباطی در جهان، که در اختیار همه افراد و سازمان‌ها قرار دارند، موارد اخلاقی و اجتماعی بسیاری را ایجاد کرده است. حال این پرسش مطرح است که چه کسی مسئول این جریان اطلاعاتی است؟ (صرافی نژاد و علی پناهی، ۱۳۸۰ : ۳۳۴)

سیستم‌های اطلاعات می‌توانند به‌شکل مستقیم یا غیر مستقیم روی فرهنگ ملی یک جامعه تاثیر بگذارند. این تاثیر می‌تواند اخلاقی (اشاعه فساد، عکس، فیلم و گروه‌های ضد اخلاقی)، عقیدتی (فعالیت سایت‌های علیه ارزش‌های بنیادین و ارکان اعتقادی یک جامعه) و اجتماعی (فعالیت‌های جدید برای ایجاد خرده فرهنگ‌ها که منجر به تخریب بنیادهای اجتماعی و فرهنگی جوامع می‌شود) باشد (ربیعی، تقریرات درسی دکتر ربیعی در درس مدیریت بحران‌های ارتباطی، دانشکده علوم اجتماعی دانشگاه تهران، 1388).

۳-۲ بحران فرهنگی

بسیاری از نتایج منفی سیستم‌های اطلاعاتی تنها تجاوز به حقوق فردی افراد و یا تجاوز به حق مالکیت آنها نیست، بلکه زیان‌هایی است که می‌تواند بر افراد، جوامع و نهادهای سیاسی وارد کند و عناصر یا ارزش فرهنگی و اجتماعی را تخریب کند (ثاقب تهرانی و تدین، ۱۳۸۴ : ۳۳۹).

یکی از لوازم رو در رویی فرهنگ ملی و سنتی با فرهنگی که به همراه فنآوری به‌شکل تهاجمی وارد می‌شود، بحران فرهنگی است که در راس آن عوارضی چون آلودگی محیطی، روانی، سستی اخلاقی، عدم اعتماد و بدبینی نسبت به سازمان‌های موجود، از خود بیگانگی، عصیان جوانان و بی‌اعتبار شدن ارزش‌های سنتی قرار دارند (مدد پور، ۱۳۷۲ : ۴۲).

۳-۳ شکاف نسلی

فیس بوک‌ها و خدمات اینترنتی که در ابتدا فقط برای جوانان طراحی شده بودند، در نهایت مورد هجوم بزرگسالان قرار گرفتند. این امر خود منجر به پیدایش یک‌سری هنجارهای اجتماعی جدید شد. زمان، پیامدهای این تغییر اجتماعی را مثل همه موارد دیگر برای جوانان به امری عادی تبدیل خواهد کرد. مثلا وجود دوربین‌های مدار بسته برای یک شهروند جوان امری عادی تلقی شده و می‌تواند گسترش این دوربین‌ها را در فضاهای عمومی تایید کند و به ضمایم زندگی مدرن بیفزاید اما تلقی این امر به‌سان امری عادی برای سالمندان و بزرگسالان دشوار است (شریفیان ثانی،۱۳۸۷ : ۹۸).

در ایران هم، گرایش جوانان به این خدمات اینترنتی بالا بوده و این امر منجر به شکل‌گیری شکاف‌های ارزشی عمیقی شده است (اخوان صراف، ۱۳۸۵: ۲۸).

۳-۴ شکاف دیجیتالی

اگرچه ورود به عصر نوین، اطلاعات را به منبعی غنی تبدیل کرده است، اما فنآوری‌هایی که امکان دسترسی به اطلاعات را فراهم می‌کنند به‌طور یکسان میان گروه‌های مختلف مردم تقسیم نشده‌اند. برای عده‌ای، اطلاعات همچنان منبعی کمیاب است که آنان را در نابرابری نسبی اقتصادی و اجتماعی قرار می‌دهد. از تفاوت در فنآوری به‌طور عام و فنآوری کامپیوتر به‌طور خاص، میان کسانی که از آن بهره‌مند هستند و آنان که بی‌بهره اند، با اصطلاح شکاف دیجیتالی یاد می‌شود. هر چند تفاوت‌های میان اقشار ضعیف و قوی در استفاده از کامپیوتر و خط اینترنت پر سرعت به مساله شکاف دیجیتالی تا حدی دامن می‌زند اما شاید بالا بردن سواد فنآوری، درصدی از این پدیده را کاهش دهد (استیسی و برایان، ۱۳۸۶: ۳۸۳) .

۳-۵ چند زبانی در اینترنت

هنگامی که تاثیر تلویزیون با تاثیرات صنعت چاپ طی قرون گذشته مقایسه می‌شود، در می‌یابیم که با کمک اینترنت امکان تفکر مشترک درباره یک موضوع به‌طور هم‌زمان برای میلیون‌ها انسان فراهم می‌شود. این تفکر مشترک در وهله اول نوعی هویت اجتماعی در سطح جهان است که رفته رفته به هویت ملی تبدیل می‌شود. باید توجه داشت که این کارکرد در مورد همه زبان‌ها یکسان نیست. فقط زبان‌هایی که دارای پشتوانه فرهنگی و ادبیات غنی باشند، پایدار باقی می‌مانند و سایر زبان‌ها رفته رفته رو به زوال و نیستی می‌گذارند (در بیگی، ۱۳۷۹ : ۲۹۳).

۴- تهدیدات اخلاقی

۴-۱ غیر انسانی شدن و تاثیرات روانشناختی(افسردگی، تنهایی و مواردی از این قبیل)

یکی از انتقادات وارده بر سیستم‌های پردازش اطلاعات، ماهیت غیر فردی و امکان غیر شخصی کردن فعالیت‌هایی است که کامپیوتری می‌شوند. بسیاری از مردم به علت کامپیوتری شدن، احساس از دست دادن هویت خود و غیر انسانی شدن می‌کنند. انسان‌ها حس می‌کنند با آنها همانند عدد برخورد می‌شود. به‌طور کل بیم آن می‌رود که اینترنت، اثر منزوی کننده بیشتری نسبت به آنچه تلویزیون ایجاد کرده بود، داشته باشد. اگر مردم تشویق شوند که از اتاق‌های خانه خود، کار یا خرید کنند، امکان بروز اثرات سوء روانشناختی مانند افسردگی و تنهایی وجود خواهد داشت (توربان و دیگران، ۱۳۸۶ : ۱۲۵۰).

بر اساس یک تحقیق در دانشگاه استنفورد، هر چه افراد، زمان بیشتری را آن‌لاین باشند، زمان کمتری برای روابط زندگی واقعی دارند و این یعنی شیوع انزواگری (استیسی و برایان، ۱۳۸۶ : ۳۸۰).

به‌طور کل کارکنانی که به‌طور فیزیکی در سازمان حضور ندارند، منزوی می‌شوند. انزوای کارکنان به دو نوع است : حرفه‌ای و اجتماعی. به لحاظ حرفه‌ای، کارکنان نگران این هستند که از دل بروند، چرا که از دیده رفته‌اند و در نتیجه از پاداش‌های سازمانی محروم بمانند. به لحاظ اجتماعی، دغدغه کارکنان از این ابت است که تعامل غیر رسمی با همکاران و دوستان خود را از دست خواهند داد (کاپلان[۱۳]، 2008).

۴-۲ کاهش ارزش‌های اخلاقی و گسترش عدم اعتماد

اینترنت به‌دلیل ماهیت ویژه خود، محیط بسیار مناسبی برای پردازش اطلاعات حساس است چرا که نه فنآوری و نه قانون نمی‌توانند از آن محافظت کنند. در این موقعیت جوامع اطلاعاتی آینده، بیشتر از امروز در معرض خطر خواهند بود و میزان اهمیت حقوق فردی کمرنگ تر از امروز خواهد شد (دربیگی، ۱۳۷۹ : ۲۷۹).

سیستم‌های نظارتی فراگیر می‌توانند حق مصونیت از مزاحمت‌های شخصی غیر معمول را به کلی زیر پا بگذارند. این امر منجر به بی‌اعتمادی می‌شود. نزدیک به ۸۰٪ از شرکت‌های ایالت متحده کارکنان خود را به‌طور الکترونیکی کنترل می‌کنند. در انگلیس، بیش از چهار میلیون دوربین ویدئویی توسط نهادهای وابسته به شهرداری‌ها نصب شده‌اند که مردم را خارج از خانه‌ها و محل کارشان می‌پایند. در واقع یک بازدید کننده معمولی از لندن به‌طور متوسط در یک روز حدود ۳۰۰ مرتبه توسط دوربین‌ها مشاهده می‌شود (توربان و دیگران، ۱۳۸۶ : ۱۲۶۹).

۴-۳ هرزنامه[۱۴]

پخش هرزنامه عبارت است از پخش بی‌رویه پیام‌های ناخواسته از راه پست الکترونیک که در اینترنت یکی از شایع‌ترین شکل‌های پارازیت اطلاعاتی است. در واقع یک نامه الکترونیکی نا-خواسته با یک پیغام کم‌ارزش است که به‌شکل تبلیغ یا یک‌سری نامه‌های زنجیره‌ای است. سرعت بالا و هزینه کم فنآوری‌های مدرن اطلاعاتی از علل افزایش این پارازیت‌ها است. گزارش شده است که هرزنامه، حدود ۴۰٪ از تمام نامه‌های الکترونیکی را شامل می‌شود. هرزنامه‌ها آن-قدر مزاحمت ایجاد می‌کنند که اعضای اتحادیه اروپا به ممنوع کردن انبوه نامه های الکترونیکی که هرزنامه‌ها هم جزئی از آن هستند، رای داده‌اند (استیسی و برایان، ۱۳۸۶ : ۸۷).

۴-۴ وابستگی و آسیب‌پذیری

[13] Caplan
[14] spam

امروزه کسب و کارها، دولت، آموزشگاه‌ها و سازمان‌های خصوصی و حتی عبادتگاه‌ها، در فعالیت-هایشان به نظام اطلاعات وابسته شده‌اند. با همه‌جا حاضر بودن رایانه و نظام اطلاعات، باید رفته رفته بپذیریم که این پدیده نیز مانند تلفن، رادیو، تلویزیون و دیگر فنآوری های همگانی، از نظارت نزدیک و استانداردهای همه‌پذیر بر کنار است. با گسترش شبکه‌های ملی و سراسری جهانی، نیاز به استاندارد و پایش‌های پیشگیری از اشتباه، روز به روز افزایش می‌یابد (لاودن،۱۳۷۷ : ۴۴۹).

در حال حاضر، پردازش اطلاعات یک فعالیت مهم اجتماعی است. برای نمونه ۸۰٪ وقت مدیران اجرایی، به پردازش و انتقال اطلاعات سپری می‌شود (رضاییان،۱۳۸۱ :۷).

۵- تهدیدات اجتماعی ـ اقتصادی

۵-۱ ترس از دست دادن شغل

استفاده از تجارت الکترونیکی و سیستم‌های اطلاعات، منجر به حذف مدیران میانی و تنی چند از کارکنان شرکت مانند مشاغل واسطه‌ای می‌شود (واتسون[15]، 2006). روشی که با این کارکنان غیرضروری، رفتار می‌شود، ممکن است باعث پیش آمدن مسائل اخلاقی، مثل چگونگی این جابه جایی یا وجود و عدم وجود برنامه‌های بازآموزی شود. این امر خود منجر به عدم احساس امنیت اقتصادی و ترس می‌شود. ترس، یک پدیده اجتماعی است و کشورها باید نسبت به این پدیده طبیعی خطرناک که مدام در حال افزایش است، حساسیت به خرج بدهند (فانک ، 2005).

البته سخن گفتن از آثار فنآوری اطلاعات بر مجموعه مشاغل، امر دشواری است. چرا که فنآوری اطلاعات در عین اشتغال‌زدایی، اشتغال‌زا هم هست (فهیمی ، ۱۳۸۲: ۱۳۲).

۵-۲ سرقت هویت

در طی این عمل، مجرم (سارق هویت)، خود را به‌سان شخص دیگری جا می‌زند. سارق، با استفاده از شماره‌های ملی و شماره‌های کارت اعتباری افراد که معمولا از راه اینترنت به‌دست می‌آورد، به تقلب دست می‌زند (مانند خرید محصولات یا استفاده از خدمات) و قربانی ناچار است بابت آن، پول بپردازد. در دنیای مجازی، از ابزار تایید هویت خبری نیست. زیرا تایید هویت، فنآوری خاصی می‌طلبد که در سطح گسترده و عام استفاده نمی‌شود(ساروق فراهانی،۱۳۸۷ :۶).

حق مالکیت فکری از جمله عوامل هویت هر فرد است. حق مالکیت فکری به‌سان نوعی دارایی نامشهود تلقی می‌شود که افراد یا سازمان‌ها تولید می‌کنند. فنوری اطلاعات حمایت از حق مالکیت فردی را مشکل کرده است زیرا اطلاعات کامپیوتری را به‌آسانی می‌توان روی شبکه‌ها کپی و یا توزیع کرد (علی پناهی، ۱۳۸۸ : ۳۳۷).

۵-۳ حمله برنامه‌نویسی

[15] Watson

این کار توسط مجرمان کامپیوتری انجام می‌شود که فنون برنامه‌نویسی برای تغییر یک برنامه کامپیوتری به‌شکل مستقیم یا غیر مستقیم را می‌دانند. در این قبیل جرم‌ها، مهارت‌های برنامه نویسی و شناخت سیستم‌های هدف ضروری است. مثال‌هایی از این برنامه ها شامل ویروس[۱۶]، کرم[۱۷]، اسب تراوا[۱۸]و مواردی از این قبیل هستند (توربان و دیگران، ۱۳۸۶ :۱۱۵۹).

۵-۴ حمله از طریق مودم

در بسیاری از شرکت‌ها، کارکنانی که در خارج از شرکت هستند برای دسترسی تلفنی به شبکه-های داخلی شرکت از مودم استفاده می‌کنند. مودم‌ها در دو نوع مجاز و غیر مجاز است. نوع دوم زمانی توسط کارکنان نصب می‌شود که مودم مجاز در دسترس نباشد، به کارگیری آن دشوار باشد یا مودم‌های مجاز دسترسی محدودی را فراهم کنند.

مودم‌ها بسیار پر خطر هستند. نفوذ به آنها برای مهاجمان آسان است و کارکنان می‌توانند به-راحتی اطلاعات مخفیانه شرکت را از راه مودم‌های غیرمتعارف به شبکه‌های خارجی بفرستند (توربان و دیگران، ۱۳۸۶ : ۱۱۶۲).

۵-۵ بیکاری عمومی ناشی از اتوماسیون

جانشین شدن ماشین‌ها به‌جای میلیون‌ها کارگر به بیکاری عمومی منجر می‌شود. ربات‌ها و سیستم‌های اتوماسیون اداری، به‌صورتی موثر با انسان‌ها برای مشاغل یقه آبی و دفتری رقابت می‌کنند. البته باید اذعان کرد که مشاغل یقه سفید نیز از تاثیر فنآوری اطلاعات مصون نیستند. در حقیقت، ماشین‌ها چالش خود را با دانشمندان، مترجمان، برنامه‌نویسان کامپیوتر، حقوقدانان، خلبانان هواپیما و سایر متخصصین آغاز کرده‌اند (ربیعی، تقریرات درسی دکتر ربیعی در درس مدیریت بحران های ارتباطی، دانشکده علوم اجتماعی، دانشگاه تهران، ۱۳۸۸).

۵-۶ گسترش سانسور

به موازات گسترش تعداد روزنامه‌های الکترونیکی و تارنماهای خبری، سانسور مطالب آنان توسط دولت‌ها نیز رو به افزایش است. شواهد محکمی نشان می‌دهد که افراد در انتخاب و استفاده از داده‌ها و اطلاعات، دچار انحراف می‌شوند. این انحراف بر اثر شیوه‌های موجود در دسترس و پیش داوری هاست. در واقع در یک دیدگاه کلان‌تر، دولت‌ها آن دسته از اطلاعاتی را که مطابق با معیارهای خود و صلاحدیدشان نیست، سانسور می‌کنند (ثاقب تهرانی و تدین، ۱۳۸۰ : ۱۱۲).

۵-۷ پیدایش مشکلات حقوقی

---

[16] Virus
[17] Worm
[18] Trojan horse

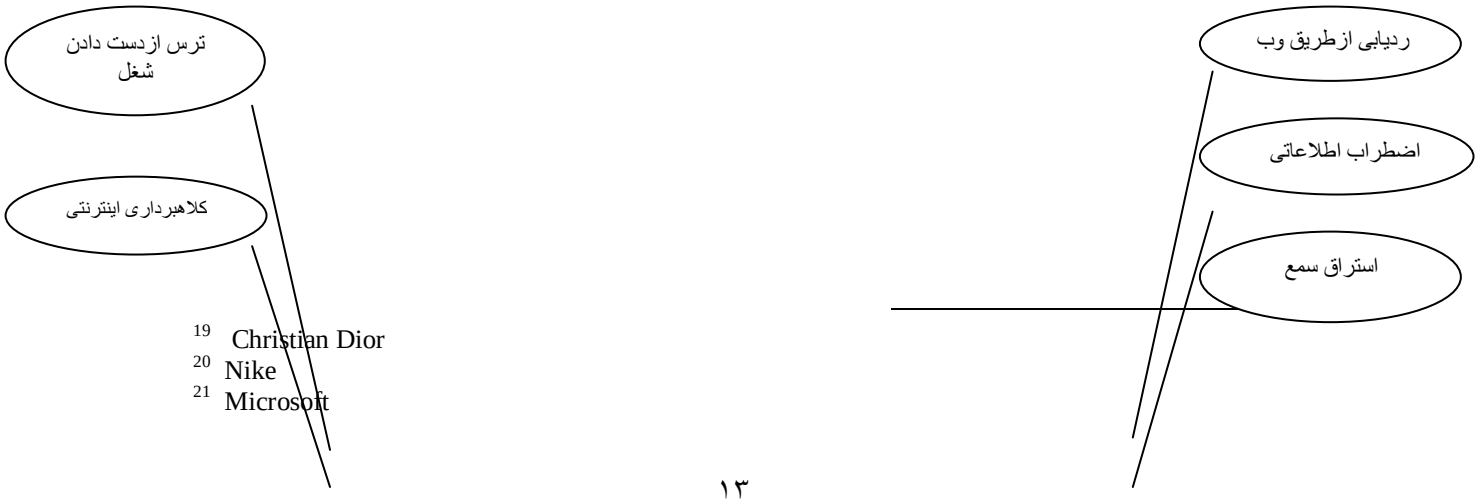
قوانین حاکم بر تجارت الکترونیک اغلب وجود ندارند یا تازه نوشته شده‌اند. قانون‌گذاران، دادگاه-ها و توافق‌امه های بین‌المللی باید درباره مسایل حل نشده‌ای چون قوانین و اجرای قراردادها، تماس‌های پست الکترونیکی، نقش امضای الکترونیک و کاربرد قانون حق مولف برای اسناد الکترونیکی، راه حل مناسبی ارایه دهند (سی لاودن، ۱۳۸۰ : ۱۷۱).
در مقابل سازمان‌ها نیز قادر به پاسخگویی به‌موقع به موج‌های ایجاد شده از ورود فنآوری نشده‌اند و تدوین قوانین و نهادینه کردن آن و تسری آن در جامعه سال‌ها به‌طول می‌انجامد (صرافی نژاد و علی پناهی، ۱۳۸۰ : ۳۳۳).

۸-۵ کلاهبرداری در اینترنت (احتکار اینترنتی)
هنگامی‌که خریداران و فروشندگان یکدیگر را نمی‌شناسند و حتی نمی‌توانند همدیگر را ببینند، این احتمال وجود دارد که افراد متقلب، مرتکب کلاهبرداری یا سایر جرم‌ها از راه اینترنت شوند. کلاهبرداری اینترنتی و پیچیدگی آن به‌سرعت و حتی سریع‌تر از خود اینترنت رشد کرده است (برج و گری‌گراد، ۱۳۷۱: ۲۲۴).
در این میان شرکت‌های بزرگی مثل کریستین دیور[۱۹]، نایک[۲۰] و حتی مایکروسافت[۲۱] مجبور شدند برای به‌دست آوردن نام دامنه‌ای که با اسم شرکت آنها همخوانی دارد، رقابت کرده و یا هزینه‌های هنگفتی بپردازند.
احتکار اینترنتی به عمل ثبت اسامی دامنه به‌منظور فروش آنها به قیمت بالاتر در آینده اطلاق می‌شود. قانون ضد احتکار اینترنتی و حمایت از مصرف‌کننده، به صاحبان اسامی تجاری در آمریکا اجازه می‌دهد که در مورد خسارت‌های کیفری، شکایت کنند (توربان و دیگران، ۱۳۸۶ : ۳۱۸).

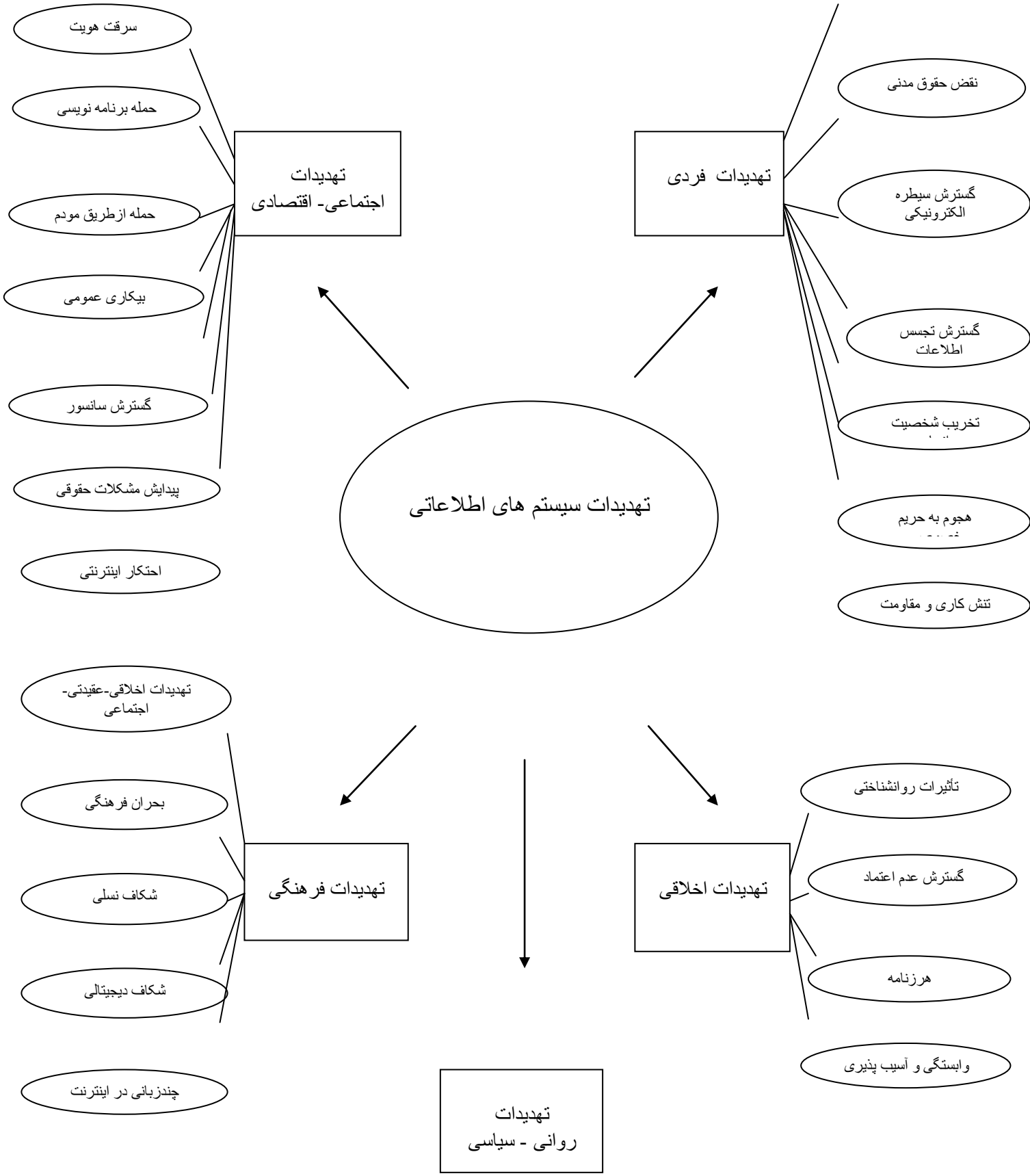
مدل مفهومی تحقیق

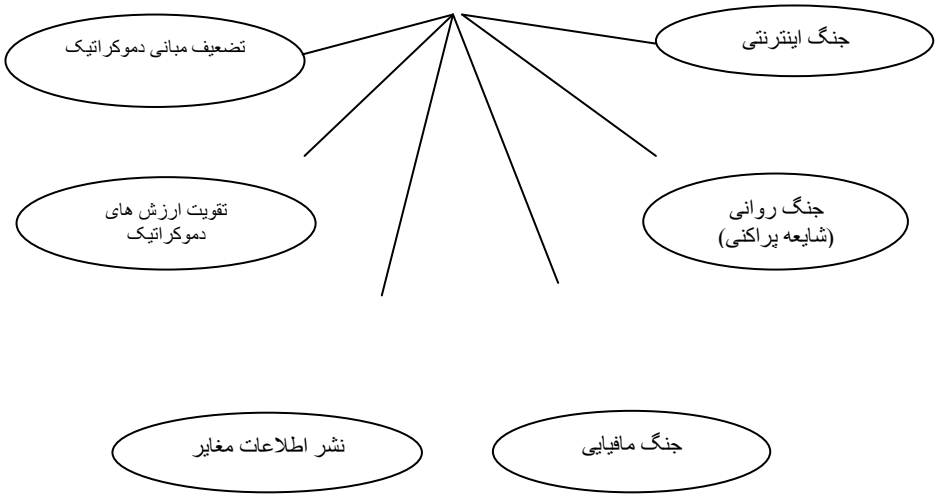
با عنایت به اهداف در نظر گرفته شده برای تحقیق و براساس دسته‌بندی عوامل تهدیدات سیستم‌های اطلاعاتی، پنج عامل مهم در مدل ارایه شده در شکل ۱، مشخص شده است.

شکل ۱. مولفه‌های تهدیدات سیستم‌های اطلاعاتی



[19] Christian Dior
[20] Nike
[21] Microsoft


تهدیدات سیستم های اطلاعاتی
تهدیدات فردی
نقض حقوق مدنی
گسترش سیطره الکترونیکی
گسترش تجسس اطلاعات
تخریب شخصیت
هجوم به حریم
تنش کاری و مقاومت
تهدیدات اجتماعی- اقتصادی
سرقت هویت
حمله برنامه نویسی
حمله ازطریق مودم
بیکاری عمومی
گسترش سانسور
پیدایش مشکلات حقوقی
احتکار اینترنتی
تهدیدات اخلاقی
تأثیرات روانشناختی
گسترش عدم اعتماد
هرزنامه
وابستگی و آسیب پذیری
تهدیدات فرهنگی
تهدیدات اخلاقی-عقیدتی- اجتماعی
بحران فرهنگی
شکاف نسلی
شکاف دیجیتالی
چندزبانی در اینترنت
تهدیدات روانی - سیاسی



روش تحقیق

روش تحقیق حاضر از جنبه هدف، کاربردی و نیز توسعه‌ای و از نظر ماهیت، توصیفی پیمایشی است. این پژوهش به مطالعه تهدیدات مهم سیستم‌های اطلاعاتی و همچنین تحلیل بالاترین تهدید احساس شده از سوی شهروندان تهرانی می‌پردازد.

در این تحقیق به جهت اینکه ماهیت جامعه آماری باید در ارتباط با سیستم‌های اطلاعاتی باشد، جامعه آماری از بین شهروندان تهرانی انتخاب شده است و به‌دلیل نا محدود بودن حجم جامعه، به‌شکل نمونه‌برداری تصادفی طبقه‌ای، تعداد ۳۳۰ نفر به‌عنوان حجم نمونه برگزیده شده‌اند.

در این تحقیق برای جمع‌آوری داده‌ها از طرح پرسشنامه استفاده شده است. این پرسشنامه شامل سه بخش است:

الف) تعاریف واژه‌ها و بیان مساله تحقیق.

ب) مشخصات پاسخ‌دهنده: در این بخش سوالاتی از قبیل جنسیت، سن، تحصیلات و شغل درج شده است.

ج) سوالات اصلی و تخصصی تحقیق: با توجه به چارچوب مشخص شده برای تحقیق و هرکدام از شاخص‌ها و بر مبنای طیف لیکرت، پرسشنامه دارای پرسش بسته و باز است. به‌منظور برآورد پایایی یا قابلیت اعتماد پرسشنامه از روش آلفای کرونباخ به‌وسیله نرم افزار اس‌پی‌اس‌اس استفاده شده است. آلفای کرونباخ برای این پرسشنامه ۰,۷۶۵ است. همچنین برای سنجش روایی و یا اعتبار پرسشنامه اقداماتی از قبیل دریافت نظرات اصلاحی خبرگان صورت گرفته است.

یافته‌های تحقیق

از بین ۳۳۰ نفر از افرادی که به پرسشنامه پاسخ دادند، ۵۳٪ مرد و ۴۷٪زن بودند. از بین آنها، ۱۲٪ دیپلم، ۱۷,۵٪ کاردانی، ۵۲,۵٪کارشناسی و ۱۸٪ کارشناسی ارشد بودند. در میان

پاسخگویان ۲٪ زیر ۱۹ سال، ۱۸٪ بین ۱۹-۲۵ سال، ۷۷٪ بین ۲۵-۴۵ و ۳٪ بیشتر از ۴۵ سال سن داشتند.

یافته‌های استنباطی تحقیق نشان می‌دهند، از میان تهدیدات ارائه شده، تهدیدات سیاسی با ۵۲,۶٪ بیشترین نوع تهدید احساس شده از نقطه نظر پاسخگویان بوده است. بعد از آن تهدیدات فردی با ۲۳,۸٪ بالاترین تهدید احساس شده است. تهدیدات فرهنگی نیز با ۲۰٪ و تهدیدات سازمانی با ۱۰,۵٪ به‌ترتیب از اولویت کمتری برخوردارند.

یافته اول: از بین تهدیدات فردی، تهدیدات روانی ـ سیاسی، تهدیدات فرهنگی، تهدیدات اخلاقی و تهدیدات اجتماعی ـ اقتصادی، عوامل سیاسی و تضعیف مبانی دموکراتیک و همچنین سانسورهای دولتی به‌سان بالاترین تهدید احساس شده توسط پاسخ‌گویان در نظر گرفته شده است. از طرف دیگر تهدیدات سازمانی، در قالب کنترل و نظارت‌های مدیران ارشد و کنترل نامه-های الکترونیکی توسط آنها، کمترین تهدید احساس شده از طرف پاسخگویان است.

یافته دوم: در بین پاسخگویان، حدود ۳۵٪ از آنها وابستگی خود را به اینترنت و سیستم‌های اطلاعاتی موجود در سازمانشان، بسیار زیاد می‌دانند.

یافته سوم: بر اساس آزمون فریدمن رتبه‌بندی تهدیدات فنآوری اطلاعات به ترتیب اولویت، تهدیدات سیاسی، تهدیدات فردی، تهدیدات فرهنگی و تهدیدات سازمانی هستند.

آزمون رتبه‌بندی فریدمن به قرار زیر است :

تهدیدات فردی	۲,۵۳
تهدیدات سازمانی	۱,۷۲
تهدیدات سیاسی	۳,۴۳
تهدیدات فرهنگی	۲,۳۲

یافته چهارم: در بین انواع تهدیدات فردی، ردیابی با وب بالاترین تهدید احساس شده است. در این میان دستیابی به اطلاعات شخصی در بین گویه‌های تهدیدات فردی، کمترین تهدید احساس شده است.

یافته پنجم: در بین انواع تهدیدات سازمانی، استراق سمع به‌سان بالاترین تهدید احساس شده است. در واقع افراد احساس می‌کنند در داخل سازمان‌ها، توسط مدیران ارشد تماس‌های تلفنی شان کنترل می‌شود.

یافته ششم: در بین انواع تهدیدات فرهنگی، تهاجم فرهنگی از راه مشاهده سایت‌های مختلف و همچنین دسترسی آسان به افراد متعدد با فرهنگ‌های مختلف، به‌سان بالاترین تهدید احساس شده محسوب می‌شود. در این میان اگر هر کشوری در زمینه شناساندن فرهنگ غنی و اصیل خود کوتاهی کند، از سایرین عقب مانده و فرهنگ کشورهای فعال در این زمینه غالب می‌شود و در راستای آن، بحران‌های متعدد اجتماعی در جوامع در چارچوب تضاد فرهنگی شکل می‌گیرد.

نتیجه گیری و پیشنهاد :

در دنیای پیچیده امروز که استفاده از کامپیوتر به‌سان عضوی جدایی‌ناپذیر از انسان‌ها گسترش یافته است، سیستم‌های اطلاعاتی متعدد و متنوعی به‌منظور تسهیل ارتباطات در بین افراد شکل گرفته‌اند. این سیستم‌های اطلاعاتی باوجود فوایدی که دارند، امنیت فردی افراد را تهدید می-کنند، آزادی‌های افراد را محدود می‌کنند و تهدیداتی پیرامون حریم خصوصی افراد مطرح می-کنند. برای مطالعه این موارد تهدیدآمیز، ما در گام اول موارد این تهدیدات را به تفکیک منشا فردی، فرهنگی، اقتصادی و غیره طی یکسری مطالعات نظری به‌دست آوردیم. در گام دوم با چند تن از اساتید و خبرگان سیستم و فنآوری های اطلاعاتی، مصاحبه‌های باز انجام دادیم تا مواردی که از قلم افتاده‌اند، افزوده شود. در گام سوم، پس از جمع‌آوری اطلاعات و دسته‌بندی آنها، پرسشنامه‌ای طراحی کرده و در سطح کاربران اینترنت و سیستم‌های اطلاعات توزیع کردیم. فنآوری‌های اطلاعاتی از لحاظ شغلی، تجاری و اقتصادی کمک زیادی به افراد کرده‌اند. اکنون بسیاری از کارها با سرعت بیشتری انجام می‌شوند گویی که این فنآوری‌ها لازمه زندگی امروزی هستند. سیستم‌های اطلاعاتی، تغییرات شگرفی در بخش‌های مختلف اجتماعی، فرهنگی، اقتصادی و سیاسی ایجاد کرده‌اند و جوامع آینده به‌شدت متکی بر سیستم‌های فنآوری اطلاعات خواهند بود. با این وجود نباید تبعات منفی این سیستم‌ها را نادیده گرفت و برای کاهش این آثار منفی باید چاره‌ای اندیشید. این تبعات منفی در کشورهای در حال گذار از وضعیتی متفاوت برخوردارند و دوگانگی متعددی چه از جنبه سبک زندگی و چه از جنبه موضوعات اخلاقی – اجتماعی به‌وجود آورده است. بنابرین مطالعه در مورد این آسیب‌ها الزامی است.

به‌سان اولین گام، قبل از پیاده‌سازی هر سیستم اطلاعاتی، باید یک برنامه استراتژیک طراحی شود، به گونه‌ای که تبعات متعدد فردی، اجتماعی، اخلاقی، اقتصادی و سیاسی پیاده‌سازی این سیستم‌ها، پیش‌بینی و طراحی‌های لازم انجام شود. داشتن یک برنامه استراتژیک، منجر می‌شود که تهدیدات را از ابتدا پیش‌بینی کرده و تا حدودی از تبعات منفی آن کاسته شود. به‌سان گام دوم که به نظر می‌رسد اصلی‌ترین گام باشد، با توجه به کشورهای مشابه ایران، فرهنگ‌سازی برای استفاده از این امکانات، ضرورتی اجتناب‌ناپذیر است. این مساله چه از جنبه آسیب‌شناسی و چه از جنبه فرهنگ نحوه کار با سیستم‌های اطلاعاتی، باید مورد توجه قرار گیرد.

براساس یافته‌های به‌دست آمده از این تحقیق، می‌توان نتایج زیر را برداشت کرد:

۱- گسترش فنآوری های اطلاعاتی باعث گسترش حوزه‌های مکانی و حوزه‌های عمل افراد شده است. بسیاری از شیوه‌های سنتی همگرایی اجتماعی مانند خانواده و گروه دوستان اهمیت خود را به‌شدت از دست داده‌اند. اجتماعات سنتی تضعیف شده و گونه‌های جدیدی از اجتماعات مجازی ایجاد شده است که پیامد آن جدایی افراد در وضعیت رو در رو و در دنیای واقعی است. این امر چیزی جز انزوا و گوشه‌گیری و فرار از محدودیت‌های اجتماعی دنیای واقعی نیست.

۲- با گسترش سیستم‌های اطلاعاتی، آزادی فردی انسان‌ها تخریب شده و حریم‌های خصوصی بیشتر در معرض دید همگان قرار می‌گیرد. بالطبع، هر فردی تمایل دارد تنها بخش محدودی از هویت شخصی‌اش افشا شود ولی با گسترش دوربین‌های شهری، استفاده از کارت‌های اعتباری و امکان کنترل افراد با تحلیل موارد خرید، مکان‌های خرید، جی‌پی‌اس ها و مواردی از این قبیل منجر به در هم ریختن مرزهای حریم خصوصی شده است.

۳- سیستم‌های اطلاعاتی به لحاظ فردی، به‌شدت فردگرایی را تقویت کرده‌اند. زیرا نگاه انسان‌ها به زندگی را تغییر داده و در نهایت افراد به درک متفاوتی از امنیت، کار، زندگی شخصی و دوستان دست می‌یابند.

۴- بر مبنای نظریه نظارت و کنترل کامل در دنیای مجازی و اطلاعاتی، آی‌پی های کامپیوترها به سادگی قابل پیگیری است و اطلاعات مخابره شده و دریافت شده به‌سادگی قابل دسترسی و بازیابی هستند که امکان تجاوز و سوء استفاده از حریم خصوصی افراد را ایجاد می‌کنند.

۵- یکی از تبعات فرهنگی سیستم‌های اطلاعاتی، این است که با وجود هم‌جنس بودن فکر و زبان، زبان نامه‌نگاری در اینترنت عوض شده و اصول یک زبان و دستور سخن گفتن و نوشتن متن کاملا تغییر کرده است.

۶- از دیگر تبعات فرهنگی، اشاعه فرهنگ‌های متعدد از راه این سیستم هاست. هرچند این امر می‌تواند آثار مثبت بالایی داشته باشد اما اگر کشوری در زمینه اشاعه فرهنگ خود و شناساندن فرهنگ ملی خود کاری انجام ندهد، هجوم فرهنگ‌های بیگانه، منجر به لطمه زدن به فرهنگ ملی و ایجاد دوگانگی و تضاد می‌شود.

۷- شاید بتوان گفت که در حوزه‌های محیطی، فنآوری های اطلاعاتی با آسان کردن ارتباطات باعث کاهش ترافیک و آلودگی هوا، و شکل‌گیری انرژی، تولید و فروش مجازی شده‌اند. اما این هشداری است مبنی بر اینکه استثمار طبیعت به استثمار " خود " تبدیل می‌شود.

۸- افزایش سانسور اطلاعاتی و گسترش عرصه‌های مورد سانسور، منجر به واکنش‌های ذهنی منفی در بین افراد جامعه خواهد شد. مقاومت در برابر سانسور، پدیده‌ای ملموس در جوامع با سانسور گسترده است. استفاده از فیلترشکن های متعدد برای دستیابی به اطلاعات، بخشی از فعالیت کاربران در اینگونه کشورهاست.

۹- از طرف دیگر سانسور اطلاعات و انتخابی کردن اطلاعات ارائه شده به افراد جامعه، موجب بی-اعتمادی در افراد می‌شود. در واقع، نوعی از نظام‌های محدود کننده را در ذهن مخاطبین متبادر می‌کند و بازتاب سیاسی هم خواهد داشت.

۱۰- در چارچوب تهدیدات سازمانی، یکی از تبعات منفی سیستم‌های اطلاعاتی، کنترل بیش از حد بر افراد و کارکنان است. می‌دانیم که از موارد مهم سیستم‌های مدیریتی جدید، دادن آزادی عمل به مدیران و زیردستان است تا بتوانند در چارچوب آن خلاقیت‌های خود را شکوفا کنند. اما در لوای این آزادی ظاهری با کنترل‌های شدید، همه چیز یک کارمند در دسترس صاحبان سهام و مدیران است. این امرخود بی‌اعتمادی را به همراه می‌آورد.

منابع:

منابع فارسی :

احمدیان راد، حمید (۱۳۸۷)، **"خلافکاران میهمان بچه‌های ما (تهدیدات IT نسبت به کودکان و نو جوانان)"**، در: ***فنآوری اطلاعات***،دوره دوم، شماره ۸۷،ص ص ۸-۱۵.

اخوان صراف، احمد رضا (۱۳۸۵)، **"مدیریت تغییر برای اجرای فنآوری اطلاعات "**، در: ***ماهنامه تدبیر***، سال هفدهم، شماره ۱۷۳ ، ص ص ۲۷-۳۷.

استیسی، ساویر و ویلیامز برایان (۱۳۸۶). **استفاده از فن آوری اطلاعات**. ترجمه احمد خزائل. چاپ اول. تهران: انتشارات شرکت ناقوس اندیشه .

اسدی، مریم (۱۳۸۴)، **" فنآوری امنیت اطلاعات با یک دیدگاه طبقه بندی"**، در: ***فصلنامه علوم اطلاع رسانی***، دوره بیستم، پژوهشگاه اطلاعات و مدارک ایران، شماره 3و4 ، ص ص ۳۲-۳۹.

بیگدلو، مهدی (۱۳۸۳)، **"ایجاد و توسعه سیستم های اطلاعاتی"**، در: ***ماهنامه تدبیر***، شماره 150.

توربان، افرایم، دروتی لیدنر، افرایم مک لین و جیمز ترب (۱۳۸۶). **فنآوری اطلاعات در مدیریت - دگرگونی سازمان ها در اقتصاد دیجیتالی**. ترجمه حمید رضا ریاحی، پوریا قطره نبی، مهدیه توفیقی و حسین صامعی. چاپ اول، ویرایش پنجم، جلد 1و2، تهران: انتشارات پنجم.

ثاقب تهرانی، مهدی و شبنم تدین (۱۳۸۴) . **مدیریت فنآوری اطلاعات**. چاپ اول. تهران: موسسه کتاب مهر نشر.

ثاقب تهرانی، مهدی و شبنم تدین (۱۳۸۰). **مدیریت و فنآوری اطلاعات**. چاپ اول. تهران: انتشارات مرکز آموزش مدیریت دولتی.

ج برج، جان و گری گراد نیتزکی (۱۳۷۱). **سیستم های اطلاعاتی در تئوری و عمل**. ترجمه منوچهر غیبی. چاپ اول. جلد 1و2. تهران: انتشارات مرکز آموزش مدیریت دولتی.

چهار سوقی، سید کمال، هدی داورزنی و پرستو شاه سمندی (۱۳۸۶)، **" مقاومت کاربران در برابر سیستم های اطلاعاتی و راهبردهای افزایش سطح پذیرش"**، در: ***فصلنامه دانش مدیریت***، سال 20، شماره 76، ص ص ۱۵-۳۰.

دربیگی، بابک (۱۳۷۹). **چالش‌های حقوقی واجتماعی فضای رایانه‌ای**. چاپ اول. تهران:انتشارات خانه کتاب.

ربیعی، علی (۱۳۸۷)، **"رسانه های نوین و بحران هویت"**، در: ***فصلنامه مطالعات ملی***، سال نهم، شماره 4، ص ص ۹۰-۱۰۹.

ربیعی، علی (۱۳۸۸) تقریرات درس مدیریت بحران های ارتباطی، دانشکده علوم اجتماعی، دانشگاه تهران.

رضاییان، علی (۱۳۸۱). **سیستم‌های اطلاعات مدیریت (مدل‌سازی اطلاعات)**. چاپ دوم . تهران: انتشارات سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه ها(سمت).

زاهدی، شمس السادات (۱۳۸۵)، **"فنآو ری اطلاعات و کنترل در عصر اینفوکراسی"**، همایش نظارت و بازرسی کل کشور، دوره دوم، ص ص ۱۰- ۱۸.

ساروق فراهان، راضیه (۱۳۸۷)، **" دزدی هویت در IT"** ، روزنامه رسالت، شماره 6483، ص ۶.

سی لاودن ، کنت و جین لاودن (۱۳۷۷). **نظام‌های اطلاعات مدیریت سازمان و فنآوری**. ترجمه عبدالرضا رضایی نژاد. چاپ اول. تهران: انتشارات فرهنگی رسا.

سی لاودن، کنت و جین سی لاودن (۱۳۸۰). **فنآوری اطلاعات مفاهیم و کاربردها**. ترجمه حمید محسنی. چاپ اول. تهران:انتشارات کتابدار.

شریفیان ثانی، مریم (۱۳۸۷)، **"کاربردهای اینترنت"**، در: ***مجله گزیده مدیریت***، سال نهم، شماره 98، ص ص ۴۲-۵۷.

صرافی نژاد، اصغر و علی علی‌پناهی (۱۳۸۰). **سیستم‌های اطلاعات مدیریت (مفاهیم، نظریه‌ها،کاربردها)**. چاپ اول. تهران : انتشارات امیر.

علی پناهی، علی (۱۳۸۸). **سیستم های اطلاعات مدیریت**. چاپ اول. تهران: انتشارات آذرخش.

فهیمی، مهدی(۱۳۸۲)، **"فنآوری اطلاعات رویکردی نوین در اشتغال زایی(کار آفرینی)"**، در: ***ماهنامه تدبیر***، سال چهاردهم، ص ص ۱۳۲-۱۴۵.

کریمی، غلامرضا (۱۳۸۲)، **" سیستم های اطلاعاتی"**، در: ***ماهنامه تدبیر***، سال چهاردهم، ص 141.

محترمی، امیر (۱۳۸۳)، **"تأثیرات فنآوری اطلاعات بر زنجیره ارزش سازمانی"**، در: ***ماهنامه تدبیر***، سال چهاردهم، شماره 139 .

مددپور، محمد (۱۳۷۲). **درآمدی بر فنآوری اطلاعات**. چاپ اول. تهران: انتشارات تربیت.

مستأجران، علی (۱۳۷۸). **سیستم‌های اطلاعات مدیریت**. چاپ اول. تهران: انتشارات کیومرث .

مک لوید، ریموند (۱۳۷۷). **سیستم‌های اطلاعات**. ترجمه مهدی جمشیدیان و اکبر مهدی پور عطا آبادی. چاپ اول . اصفهان: انتشارات دانشگاه اصفهان.

بی‌نا (بی‌تا)، **"گام های پیاده سازی سیستم های امنیت اطلاعات (ISS)"**، در: نشریه فنی مرکز اطلاعات و مدارک علمی ، دوره دوازدهم، شماره 3.

منابع انگلیسی :

Bernstein, Gala (2006), "**The paradoxes of Technological diffusion ; Genetic Discrimination & Internet privacy**" : university of Connecticut.

caplan , Aaron H. (2008), "**Disipline for creating uncensored Anonymous Internet forums"**, Loyol law school ,Los Angeles.
Dalton C.E , King C.M, & Osmanoglu T.E.(2010). **Security architecture; Design deployment and operations.** london,MC Graw hill.
Funk,William (2004-2005)," **Intimidation& the internet " ,**lewis &clarck law school, university of heilburg.
Kravets , David (2009),"**Top Internet threats ; Censorship to warrantless surveillance" ,** Available on: www.ssrn.com.
Mannes, Aaron. (2007)," **Threats of internet"**, Available on: counterrorismblog.org.
O.Neil ,Roberth. (1998), "**Free speech on the Internet;Beyond 'Indecency' "** , uniiversity of viginia school of law.
Rothman, Jennifer.E,(2005)**," Freedom of speech & True Threats "** , Harward journal of law & public policy, loyal law school,Los Angeles.
Suborna, Baruna & saifuddin khan , Muhammad. (2009)," **The status of threats of information ; security in the banking sector of Bangladesh"** , policy request, university of daka,Available on: www.ssrn.com.
wood .S & Chaffery D.(2005). **Buisiness information management ; Improving performance using information system** .first edition,prentice hall.
Watson ,Paul joseph .(2006), "**Threats to internet freedom" ,** All too Real, prison planet.