فناوری های جدید و چالش های پیش روی استفاده از آنها در عصر واقعیت مجازی

*نجمه کاراندیش
کارشناس ارشد کتابداری – اطلاع رسانی
najmehkarandish@yahoo.com
سید آرمین ابریشمی اسکویی
کارشناس اداره فناوری های اطلاعاتی
مرکز منطقه ای اطلاع رسانی علوم و فناوری
armin112002@gmail.com

چکیده:
در طـول دهــه اول قرن ۲۱ ، جهان شــاهد انقلاب ســوم علمی و صنعتی بــوده و فناوری هــای دیجیتالی و فناوریهای اطلاعاتی زیرســاختهایی اساسی در ایجاد فنــاوری های همگرا مانند واقعیت مجازی می باشــد و این زیرساختها توســعه علوم و فناوری را تا حداقل ۵۰ ســال آینده رهبری خواهند کرد. در این مقاله ســعی بر مطالعه و بررســی زوایای مختلف دیجیتالی شدن و البته چالشــهای اســتفاده از این فناوریها برای انسان معاصر داریم. از جمله مهمترین مسائل آن مربوط است به رایانه ها و شــبکه های رایانه ای سپس مسائل مربوط به زندگی، محیط ، ســلامت و بهداشت روان و کار و در نهایت نیز به مسائل اقتصادی در محیط دیجیتال می پردازیم.

کلید واژه ها: فناوری هــای دیجیتالی؛فناوری های اطلاعاتی؛ واقعیت مجازی؛ اطلاعات محوری؛ چالشــها؛ امنیت شبکه ای

مقدمه:

در قرن بیستم میلادی انسانها شاهد گذران عصرهای اتم ، فضا ، اینفوتک و های‌تک [1] بودند. در عصر اطلاعات دیجیتال که دهه های واپسین قرن ۲۰ و دهه اول قرن ۲۱ شاهد آن هســتیم، زندگی انسانها روند اطلاعات محور به خود گرفته است.

انسان ها با داشتن اطلاعات در همهٔ زمینه‌ها و جنبه‌ها تمدن مدرن و فرامدرنی را ساخته اند و کشورهای پیشرفته و توسعه یافته در حال گذار از موج سوم [2] به موج چهارم و در حال به تحقق رســاندن نظریه های مربوط به جامعهٔ مجازی و واقعیت های مجازی هســتند. کشــورهای در حال توسعه نیز که سعی در رساندن خود به پیشرفت‌های کشــورهای توســعه یافته را دارند به مســألهٔ اطلاعات دیجیتــال توجه دارنــد و در حال ســرمایه‌گذاری‌های وسیع در این زمینه هستند(داورپناه ۱۳۷۸)؛ از جملهٔ این کشــورها، کرهٔ جنوبی است که در بین سالهای ۲۰۰۰ تا

۲۰۰٤ ماهواره‌های ارسال و دریافت امواج دیجیتال خود را در مدار زمین قـرار داد، به این ترتیب پی‌ریزی های مناسبی جهت وارد کردن و کاربرد فناوری اطلاعات در این گونه کشورها انجام شده است.

کشـور ایران نیز در تلاش اسـت که طبق برنامه های توسـعهٔ میان مدت (برنامه های توسعه ۵ ساله) و بلند مدت (برنامه ای که سند چشم انداز ۲۰ ساله ایران نشان می دهد)، فاصلهٔ توسعه زیرساخت های فناوری اطلاعات را نسبت به کشورهای دیگر دنیا کمتر کند و با استفاده از فناوری های روز دنیـا در زمینه اطلاعات و دیتا، ارتباطات راه دور و تبادل اطلاعات در سطح بین المللی به توسعه‌ای نسبتاً پایدار در اطلاعات و ارتباطات دست یابد. بنا به اذعان متخصصان ابتدا باید زیرساختهای فنی و فناوری وآموزشی و پژوهشی آن را فراهم کند و همین ایجاد زیرسـاختها چالشـی فرا روی مسئولان است. (ماهنامه وب، ۱۳۸٤)

دیجیتالی شدن و دیجیتالی کردن در دو دهه اخیر به مراکز و مؤسسـات دولتی، نیمه خصوصی – نیمه دولتی و خصوصی رسـوخ کرده و در ایـن میان کتابخانه های علمی – تحقیقاتی از این قاعده مستثنی نبوده و نیستند، آنها نیز سـعی بر این دارند تا اطلاعات چاپی مخزنشان را دیجیتال کرده و به اصطلاح کتابخانه های بدون کاغذ ایجـاد کنند، امـری که از دههٔ ۹۰ در کشـورهای دیگر مطرح بود و همهٔ مراکز و مؤسسات، اطلاعات مربوطه را در قالبهـای(xml) (html) و تحت پایگاه در آورده و آنها را در قالب صفحات وب تنظیم و به صورت آنلاین از طریق وب جهانی و رابطهای کاربری[۳] به مشـتریان و متقاضیان خدمات خـود عرضه می نمایند. روند تبدیل کتابخانـه هـا از چاپی و کاغذی بـه دیجیتالی همچنان ادامه دارد تا آنجا که گوگل بزرگ‌ترین شرکت در صحنه رقابت های تجاری شـبکه جهانی اینترنت سال گذشته اعـلام کرد که در حـال راه‌اندازی بزرگتریـن کتابخانه دیجیتال در شـبکه اینترنت است. اکنون که خصوصیات عصر سـوم را بیان داشتیم به نظریه های عصر چهارم یا عصر واقعیت مجازی نیز در همین جا به صورت اجمال اشاره ای خواهیم داشت.

در عصری کـه در ابتدای آن قرار داریم و تا سـال ۲۰۱۵ بـه اوج فناوری های خود خواهد رسـید ، عصر واقعیت مجازی نـام دارد که در آن تولید انبوه کالاهای فیزیکی محدود گشته و تولید و ارائهٔ کالاهای غیرفیزیکی مانند اطلاعات، موسیقی، فیلم و طراحی و معماری انواع بازی های رایانـه ای به بازار مصرف و طراحی و ایجاد موقعیـت های پر خطر برای انسـان در فضای مجازی، افزایش چشـمگیر خواهد یافت. به ایـن ترتیب اقتصاد جدید بر پایه های آن سـاخته خواهد شد (ماهنامه وب، ۱۳۸٤).

تمدن غرب سه عصر کشاورزی، صنعتی و اطلاعات دیجیتال را پشـت سر گذارده و اکنون در حال ورود به عصر چهارم است : عصر واقعیت مجازی.

عصر واقعیت مجازی را نظریه ی موج چهارم آلوین تافلر این گونه ترسـیم و توصیف می کند: کشـورهای دنیـا در تـلاش بـرای قدم نهـادن به آن و رسـیدن به جامعـهٔ اطلاعات، سـامانه هـای اطلاعاتـی و ارتباطی خـود را از مرحلهٔ تولید تا اسـتفاده به صورت شـبکه ای در آورده و همـه مبـادلات اطلاعاتـی و تعامـلات انسـانها در این جامعه با محیـط پیرامون خود با ابزار و فناوری‌های اطلاعات درآمیخته اسـت، بـه این ترتیب است که علومی چون ریاضیات کاربردی، سخت‌افزار و نرم‌افزار رایانه، فن‌آوری اطلاعات و ارتباطات، مهندسـی سـامانه‌های الکترونیکی و مخابراتی و هوشـمند و دیگر رشته های دخیل در این حوزه موجب پیشرفت و ارتقای زیرساختها و روسـاختهای فنآورانه در جامعهٔ اطلاعاتی می شـوند و منجر به پیشبرد آموزش و تحقیق، تجارت و بانکـداری، امور عمومی و خصوصی و امور دولتی در جامعهٔ اطلاعاتی می گردند و به تبع از بار تعاملات چهره به چهره و کاغذی کاسـته و به قابلیت های سـامانه های اطلاعاتی در دریافت و ارسال اطلاعات و پیام های افراد به یکدیگر افزوده می شود.

به این ترتیـب کتابخانه هـای دیجیتالی در جامعهٔ اطلاعات مأمن افرادی است که شبانه‌روز خود را در محل کتابخانه هسـتند، و وقت صرف کنکاش و جستجو در پایـگاه های اطلاعاتی، منابع اطلاعات چندرسـانه ای[٤]، اینترنت و سایر شبکه‌های اطلاع رسانی می کنند. به این ترتیب کتابخانه در ایـن جوامع از مکانی تک بعدی که صرفاً برای مطالعه است، خارج می شود و ابعاد دیگری پیـدا می کند. از جمله تفریح و سـرگرمی، کار و حرفه، گذران اوقات فراغت برای همه افراد در هر رده سـنی و در همه دوران زندگی و آموزش خودانگیختهٔ مادام‌العمر تا پایان زندگی. چنان که اشـاره شد، دانشجویان نیز در چنین شـرایطی در محیطهای پیش سـاخته با معماری شـبیه سازی شده با محیط واقعی و شرایط واقعی بدون هیچ خطری برخورد کرده و به کسب تجربه می پردازند به این ترتیب با بهره گیری از دسـتگاه‌ها و سـامانه‌های پیشرفته مطالب آموزشی و درسی را بهتر و عمیق‌تر فرا می گیرند و احساس اطمینان خاطر بیشتری نیز خواهند کرد. حتی دانشجویان می آموزند که چگونه در محیط های پیش سـاخته ای مشـابه محیطهای جستجوی واقعی که

به طور مثال توسط نرم افزار shock wave تهیه می گردد، اطلاعات را بازیابی کنند و به لینک های فرامتنی نیز راه یابند و اینها همه ارمغان عصر واقعیت مجازی است برای انسان . (ویلیامز، استیسی، ۲۰۰۱)

فناوری های دیجیتالی و چالشهای کاربری و استفاده از آنها :

در این مقاله سعی بر مطالعه و بررسی زوایای مختلف پارادایم نسبتاً جدید دیجیتالی شدن داریم و چالشهایی که انسان معاصر با آن روبرو است که از جملهٔ مهم ترین آنها مسائل مربوط به ایمنی رایانه ها و شبکه می باشد؛ سپس مسائل مربوط به زندگی، محیط، سلامت و بهداشت روان و کار و در نهایت نیز به مسائل اقتصادی در محیط دیجیتال می پردازیم.

● **مسائل مربوط به امنیت و تهدیدات رایانه ها و سامانه‌های ارتباطی**

از بین تهدیدهای امنیت رایانه ها به موارد زیر می توان اشاره داشت:

۱- خطاها و تصادفات، مانند خطاهای انسانی، خطاهای مربوط به طرز عمل و شیوهٔ عمل ، خطاهای نرم‌افزاری، اشکالات الکترومکانیکی و مسائل مربوط به «داده‌های آلوده».

۲- پیشامدها و حوادث طبیعی مانند زلزله ها، طوفانها و آتش سوزی ها و کشمکش‌های داخلی و حتی تروریسم شبکه ای.

۳- جرایم رایانه ای، که می توانند اعمال غیرقانونی و غیرمجاز باشند که در برابر رایانه ها رخ می دهد و یا استفاده از رایانه ها برای اجرای اعمال غیرقانونی . جرایم در مقابل رایانه ها شامل دزدی نرم افزار، سخت افزار، خدمات یا اطلاعات و یا جرایم مربوط به سوء نیت و تخریب است.

٤- جرایمی که با کاربرد رایانه انجام می شوند شامل سرقت کارت اعتباری، تقلب در سرمایه‌گذاری و جذب سرمایه و تقلبِ صِرف.

۵- کرمها ، برنامه هایی که خودشان را به صورت تکراری در حافظهٔ رایانه یا روی دیسک گردان کپی می کنند و ویروسها ، برنامه های منحط و انحرافی که روی درایو سخت ذخیره و انبار می گردند و می توانند دیتای ذخیره شده را نابود سازند. کرم ها و ویروس ها نیز می توانند با تعویض دیسکهای فلاپی آلوده یا داده‌ی آلوده که بر روی یک شبکه فرستاده می شود منتقل شوند؛ با نرم افزارهای ضد ویروس می توان ویروس ها را شناسایی و فعالیت آنها را متوقف کرد. مجرمان رایانه ای که ممکن است افراد شاغل در یک سازمان باشند، کاربران بیرونی، نفوذگران و ناقضان، متجاوزان [۵] و مجرمان حرفه ای. نفوذگران دسترسی غیرمجاز و غیرمعتبر به رایانه ها را غالباً تنها برای چالشهای آن انتخاب می کنند و کراکرها یا قفل شکنان حرفه ای برای اهداف مغرضانه و ستیزه جویانه اقدام به این اعمال می نمایند.

● **امنیت**، که عبارت از حفاظت از رایانه ها در شبکه های ارتباطی. ایمنی، سامانه تضمین امنیت و ایمنی جهت حمایت و حفاظت از رایانه ها در مقابل سوانح و بلایای طبیعی و رمزنگاری و دسترسی غیرمجاز است، ٤ مؤلفه دارد:

۱- سامانه های اطلاعاتی سعی می کنند تا کاربران مجاز و معتبر را با ۳ معیار معین کنند: با آنچه در اختیار آنهاست اعم از کلیدها، نشان ها و امضاءها، با آنچه که می دانند اعم از پین‌کدها یا شماره های شناسایی شخصی و رمز عبورها یا کدها و کلمات خاص) و یا باشخصی که خصوصیات خاصی دارد اعم از خصوصیات فیزیکی که می تواند در بیومتریک [۶] مشخص شده باشد.

۲- رمزنگاری، دستکاری و تغییر، اگر تغییراتی انجام نشود و ایمنی نیمه تمام بماند، دیتا نمی تواند قابل استفاده باشد. بنابراین تلاش می شود تا پیامها و برنامه های ایمن تری ساخته شود.

۳- نرم افزار ها و داده ها با کنترل دسترسی به پوشه ها و پرونده ها با تستهای کنترلی که برنامه های مورد استفاده را ردیابی می کند، حفاظت می شوند، و افرادی، متقاضیان صفحهٔ کاری و دیگر کاربران را کنترل می کنند.

٤- برنامه های بهبود شرایط ناگوار و حملات ویروسها، روشهایی برای بازسازی مجدد عملیات رایانه پس از تخریب یا اعمال تصادفی است.

● **مسائل مربوط به کیفیت زندگی** که به محیط ، سلامت ، بهداشت روانی و محل کار بستگی دارد. بعضی از مسائل و موضوعاتی که به فناوری اطلاعات ارتباط دارد به این قرار است:

۱- رایانه ها ممکن است مشکلات محیطی به وجود آورند مانند قرار گرفتن تعداد زیادی تجهیزات ارتباط راه دور در موقعیتهای طبیعی.

۲- مشکلات سلامت روانی که مرتبط با رایانه است که شامل انزوا، قمار و بخت آزمایی برخط و استرس است.

۳- مشکلاتی که تولیدی بودن محل کار را تحت تأثیر قرار می دهد که شامل غیرقابل استفاده شدن و از کارافتادگی فن آوری وقتی که کارمندان وقت شرکت را با اشغال خطوط برخ برای مقاصد شخصی هدر می دهند؛ دستکاری رایانه ها به دلیل مشکلات نرم افزاری یا سخت افزاری ؛ و در نهایت اضافه بارگذاری اطلاعات .

● **مسائل اقتصادی** مانند اشـتغال و فاصله طبقاتی ثروتمنـدان – فقـرا . انتقاداتـی اقتصـادی بـه فناوری اطلاعـات وارد می گردد کـه از جمله آنها: (۱) فناوری در وظایف و کارهایی که قابل محاسبه نیست، جایگزین انسـان شده و با میلیون ها نفر کارگرانی که اشتغال تمام وقت یا پاره وقت دارند یا بیکارند، روبرو هسـتیم؛ (۲) فناوری فاصلهٔ بین فقیران و اغنیاء را بیشتر کرده، فاصله بین کسـانی که ثروتمند اطلاعاتی‌اند و کسانی که از نظر اطلاعات بی چیز و فقیرند.

● **محیـط دیجیتال و بعضـی عواملی که اندازه و شکل آن را تحت تأثیر قرار داده به این ترتیب است:**

۱- زیربنای اقتصادی اطلاعات ملی یک طرح جامع و بزرگ است که به شـرکت های خصوصی و اینترنت وابسـته است. ۲- اینترنت قبلی در حال جایگزین شدن با شبکه های اینترنت جدید مانند VBNS ، اینترنت II و NGI است.پروژه VBNS جزء دولت اصلی ایالات متحـده که برای ارتقای محور اصلی یـا کانونهای اولیهٔ انتقال داده طراحی و اجرا شـده اسـت. اینترنت II یک برنامهٔ تجاری – دانشـگاهی مشـترک است که کاربران نهایی را قادر می سازد که داده ها را سریعاً انتقال دهند، با به کارگیری VBNS، نسـل بعـدی اینترنت (NGI) طوری طراحی شـده که در گره خـوردن محور اصلی فـرا اجرایی با زیربنای فدرال کمک می کند. ۳- شـبکه ارتباطات راه دور ۱۹۹٦ برای این طراحی شد تا شراکت بین تجارت و بازرگانی های از راه دور را افزایش دهد، به این ترتیب شرکت های بسیار گوناگون از ارائه خدمات متفاوت و نسبت به هم افزونتر به مشتریان محدود نمی شدند.٤- در طرح ۱۹۹۷ کاخ سـفید به دولت فشـار آورد که دولت بایـد از فضای تجارت اینترنتی خارج باقی بماند و فضا را برای رقابت شرکتهای خصوصی باز بگذارد.۵- ICANN یک مؤسسـه اینترنتی است که نامها و شماره ها را ثبت مـی کند این سـازمان غیرانتفاعی اسـت و برای ضابطه مند کردن نام های دامنه اینترنتی تأسـیس گردیده است. (ویلیامز، استیسی، ۲۰۰۱)

● IFARA. اینترنت در مسیر خود به رسانهٔ غالب تبادل اطلاعات تبدیل گردیـده و بیش از آن که یک چیز لوکس باشد مانند تلفن یک ضرورت است و اینطور می گویند که از لحاظ تحلیل آن «هر کس بدون آن در خطر خاموش شدن و برکنار ماندن است.»

پهنای این «شـکاف دیجیتالی» بین آنها کـه با و بدون دسترسی به فناوری اطلاعات هستند در حال عریض تر شدن اسـت. همچنان که عصر اطلاعات مـی رود تا تولیدات و ثروت را رونق و گسـترش دهد، این شـکاف یکی از مهم‌ترین چالشـهای زمان ما قلمداد می شود. در سطح بین المللی، شـکاف دیجیتالی بین کشورهای ثروتمند و فقیر اسـت. در ایالات متحده، ۱۰ درصد اقتصاد صرف خرید سـخت افزار و نرم افزار می شـود؛ در مقایسه با کشورهایی نظیر سری‌لانکا و بنگلادش که سهم آن یک دهـم یک درصد اسـت. از حدود یـک میلیارد صفحه وب دَر دنیـا بیش از ۸۰ درصد به انگلیسـی اسـت. با تنهـا ۵ درصد از جمعیت دنیا، ایالات متحده ۵۰ درصد رایانه های خانگی متصل به اینترنت را داراست. با اینکه در آمریکا شـمار زیادی از مردم از سیستم جدید تبادل اطلاعات با حساب در آمد پایین آنها و یا دانش محدود آنها نسبت به زبان انگلیسی، دور مانده اند.

همچنان کـه اینفوتک به دنیا هجوم آورده اسـت، شـکاف دیجیتالی تنها یکی از چالش های فراوانی است که فرا روی ما محسوب می گردد.

مسائلی که مربوط به ایمنی می گردد شامل خطرات و تهدیـدات رایانـه ها و سیسـتمهای ارتباطی اسـت . مسـائل ایمنی می رود که مرکز قابلیت کاری رایانه ها و سـیتمهای ارتباطی تبدیل گردد. خطراتی که رایانه ها و سامانه های ارتباطی را تهدید می نماید، چنین است:

● جرایمی که با اسـتفاده از رایانـه ها و ارتباطات انجام می گیرد.

-کرمها و ویروسها

- مجرمان اینترنتی

- حـوادث غیرمترقبه طبیعـی و خطاها و تصادفات غیر طبیعی و انسانی

● جرایمی که با بـه کارگیری رایانه ها و ارتباطات راه دور انجام می گیرد. همانطور که یک ماشـین می تواند در ارتکاب یا کمک در انجام یک جرم اسـتفاده گردد، فنـاوری اطلاعات هـم می تواند افزون بـر آن اغفال و تقلـب در سـرمایه‌گذاری بـه فضای سـایبر نیـز وارد شـده و کلاهبـرداری از طریق پیشـنهاد پول‌هایی برای سـرمایه‌گذاری خارجی و مشـاوره های تلفنی تقلبی و دسـتکاری قیمت های بـورس جزء این موارد اسـت. بسـیاری از مردم هم اکنون از سرویسـهای پیوسته برای ادارهٔ موجودی اوراق بهادارشان در بورس استفاده می کنند، به ازای کارمزدها و حق‌العملهایی که در قبال ارائهٔ خدمات دریافت می شـود. بازیگران نقشـه از پیش کشیده شده برای کلاهبرداری پیشنهاد پولهایی می کنند برای سرمایه گـذاری ای که وجود خارجی ندارد و با مشـاوره های تلفنی و دسـتکاری قیمتهای بـورس این اعمال خود را دنبال می کنند.

● جرایمی که در برابر رایانه ها و ارتباطات صورت

مـی پذیرد. جرائم رایانه ای می تواند به دو نوع باشـد: (۱) مـی تواند یک عمل غیرقانونی باشـد که در مقابل رایانه ها یا ارتباطات راه دور انجام می شود. یا (۲) می تواند با کاربرد رایانه یا ارتباطات راه دور برای به انجام رسـاندن یک عمل غیرقانونی باشد.

● جرایمـی کـه در برابـر فناوری هـای اطلاعاتی صـورت مـی گیرد شـامل این مـوارد اسـت : دزدی سخت‌افزار – نرم افزار یا زمان کامپیوتر، کابل یا خدمات تلفن یا دزدی اطلاعات. دیگر اعمال غیرقانونی جرایمی هسـتند که از روی غرض‌ورزی و برای تخریب انجام می گردند مانند: دزدی از سخت افزار، که می تواند در این گسـتره قرار گیرد و دامنه‌اش از سرقت لوازم جانبی از یک مغـازۀ فروش لوازم رایانه تا سـرقت یک رایانه کیفـی یا تلفن همراه از اتومبیل یک فرد باشـد. مجرمان حرفه ای ممکن اسـت قطعات چیپهـای ریزپردازنده را از یک میز بارگذاری شـده یا حتی بـا به زور باز کردن ماشینهای پول نقد کن cashier در خارج از دیوارهای یک مرکز خرید سرقت کنند.

● اریک آویلا، ۲۶ سـاله ، یک دانشجوی تاریخ در دانشـگاه کالیفرنیا در برکلی بود، رسـاله دکتری وی که شـامل ٦ سال تحقیق موشکافانه و دقیق می شد و روی درایو هارد لپ تـاپ مکینتاش خود ذخیره کرده بود را یک دزد از آپارتمانش به سـرقت بـرد. علی رغم اینکه او یک ویرایش قبلی از رسـاله خـود را کپی کرده بود، ۷۰ صفحه از رسـاله اش که عنوان آن بهشـت گمشده: سیاسـت و فرهنگ بعد از جنگ لوس آنجلس بود روی یک دیسکت ذخیره کرده بود و دزد آن را نیز به سرقت برده بود. او اذعان کرد که گیج شـده اسـت. وی گفت: حالا آن رفته و هیچ راهی نیسـت که بتواند دوباره آن را در مغزش بازسـازی کند. آنچه موضوع را وخیم تر کرد این بود که هیچ انتخابی نداشت و باید وام ۲۰۰۰ دلاری را هم بازپرداخت می کرد برای رایانه ای که آن را دیگر نداشـت. عاقلانه این است که ما روی آن تکیه کرده ایم همیشه نسخه های پشتیبان از اطلاعات و داده های مهم خـود تهیه کنیم و آن ها را در جای امن – جدا از رایانه خود قرار دهیم.

● دزدی نرم افزار. به طور کلی دزدی نرم افزار شامل کپی های غیرقانونی نرم افزار، علاوه بر سرقت دیسکهای فلاپی یک فرد به طور فیزیکی است. تولیدکنندگان نرم افزار به طور سرّی در بولتن‌بوردهای الکترونیکی در تحقیق روی تولیدات به سـرقت رفته پرسه می زنند. سپس می کوشند کـه یک حکم قضایی برای انحلال آن بولتن بوردها پیدا کنند. همین طور دنبال سازمان هایی هستند که softlift شـرکتها، دانشـکده ها ، یا دیگر مؤسسات که یک کپی از یـک برنامـه را می خرند و برای بسـیاری از رایانه ها کپـی تهیه مـی کنند. بسـیاری مانند این کـه قاچاق نرم افزارهای غیرمجاز نامیده می شـوند، گزارش می شـوند که انجمن ناشـران نرم افزار، دانشجویان را دستگیر و به پلیس نرم‌افزار تحویل داده اند. SPA (انجمن ناشـران نـرم افزار) برای گزارش تهیه کپی غیرقانونی از نرم‌افزار در آمریکا یک شـماره (۷۴۷۸-۳۸۸-۸۰۰) با خط آزاد دارد. در دهۀ ۹۰ دو دانشجوی دانشکده نیوانگلند برای آنکه گفته می شـد از اینترنت برای تشـویق معاوضه و خرید نـرم افزار دارای حق مؤلف اسـتفاده می کردند، متهم شدند.

● نـوع دیگـری از دزدی نرم افزار کپـی یا جعل برنامه های نرم افزاری شـناخته شـده و مشـهور است. این قاچاقهـا غالباً در چین، تایوان، مکزیک، روسـیه و قسمتهای مختلف در آسیا و آمریکای لاتین برنامه‌ریزی و به اجرا در می آید. در بعضی کشورها، بیشتر نرم افزار مورد کاربرد ریزرایانه های آمریکا اینطور تصور می شود که غیرقانونی کپی می شوند.

● دزدی از زمان و خدمـات. دزدی از زمان رایانه بیش از آنچه ممکن اسـت تصور شود معمول و مرسوم اسـت. احتمالاً بزرگترین نمونه افرادی هستند که زمان رایانـه بـه خدمـت گرفتۀ خـود را بـرای پرداختن به مسـابقات، انجام خرید آنلاین یا خرید و فروش سـهم (تجارت بـورس) یا فرورفتـن در هرزه‌نمایی‌های وب صـرف می کنند. بعضی از افرد مشـاغل فرعی ای را به عنوان شغل دوم خود انجام می دهند.

● سالها کسانی که مکالمات تلفنی را به شکل غیرقانونی شنود می کردند[۷]، شرکتهای تلفن را دچار مشکل کردند و راه هایی را برای دستیابی به سامانه های صدا– پیغام شرکت یافته اند، سـپس از یک خط داخلی برای مکالمه های راه دور با هزینۀ شرکت اسـتفاده کرده اند. همچنین راههایی برای راهیابی به شبکه های تلفنی سلولی و شماره گیری مجانی یافته اند.

● دزدی اطلاعات: سـارقان اطلاعات در فایلهای اداره امنیت اجتماعی رخنه کرده و رکوردهای شخصی محرمانه را دزدیده و اطلاعات را به فروش رسـانده اند. در دانشگاه ها، سـارقان اطلاعات خصوصی مانند درجات علمی را زیر نظر گرفته و آنها را به سرقت می برند.

همیـن طور سـارقان دیوارهای امنیتـی رایانه های دفاتـر اعتباری اصلی را شکسـته و وارد آن شـده‌اند و اطلاعات مالی و اعتباری افراد را به سرقت برده اند. یک سـارق که توانسته بود قفل (رمز عبور) سامانه های لوح

فشـرده خرده فروشی اینترنتی بین المللی را بشکند و به آن داخل شود، ۳۰۰۰۰۰ شمارهٔ کارت اعتباری مشتریان را دزدیـده بود. هنگامی که مأموران اجرایی شـرکت از پرداخت تقاضای باج سـرباز زدند، او آنها را به تدریج روی اینترنت برای دیگران گذاشت و فروخت تا به طور غیرقانونـی کارت خود را شـارژ کنند، تـا اینکه تمام و متوقف شد.

● جرایـم غرض ورزانه و تخریـب (نابودی). گاهی اوقات مجرمان بیشتر علاقمندند که سامانه های ارتباطات راه دور و رایانه ها را تخریب یا از آنها سوء استفاده کنند.

● بیـش از آنکه بخواهند از آنها سـود بجویند. به عنـوان مثال یک دانشـجو در یک سـایت دانشـگاهی ویسکانسـین تعمـداً و به طور مکرر سـامانه رایانه یک دانشـگاه را از کار انداخت و این باعث شد پروژه های نهایی ده ها نفر از دانشـجویان از بین برود. قاضی او را محکوم به یک سـال مجازات تعلیقی کرد و مجبور شد دانشگاه را ترک کند.

● کرمها و ویروسـها شـکلهای دیگـری از اعمال مغرضانه در فناوری برترند. کرمها برنامه هایی هسـتند کـه خود را بارها در حافظهٔ یک رایانه یا روی دیسـک گـردان کپی می کنند. گاهی اوقات آن کرمها خودشـان را کپـی می کنند که غالباً ممکن اسـت دلیلی شـود که رایانـه صدمه ببیند یا از کار بیفتد. یک مثال ملیسـا بود کـه برنامهٔ کرم در ۱۹۹۹ را کـه تقریباً یک میلیون رایانه شـخصی را تحت تأثیر قرار داد. ملیسا یک فایل مبتذل از وب سـایتهای هرزنما را در قابل پسـت الکترونیک پخش می کرد و آنها را برای افرادی که در لیست آدرس دریافت کننده ها بودند، می فرستاد. ویروسها برنامه های مخربی هستند که روی درایو هارد رایانه انبار شده و می توانند موجب آثار غیرمنتظره و غالباً ناخواسـته شوند، مانند از بین بردن و یا مخدوش کردن داده ها. پست الکترونیک مشـهور و شناخته شـدهٔ love blog که کشور فیلیپین منشـأ آن بود در ماه می سـال ۲۰۰۰ خسارتی به اندازه ۱۰ میلیارد دلار به تمام دنیا وارد آورد، این هم یک کرم و هم یک ویروس بود. یک تفاوت کرم ملیسـا این بود که سریعتر منتشر می شد و خسارات زیادی را نسبت به هـر bug دیگر قبل از آن، موجب می شـد. love bug تقریبـاً بلافاصله با یک ویروس متفاوت دنبال می شـد و نـام خود را فاش نمـی کرد اما به یک کلمه یا کلمات تصادفـی تغییر نام می داد و هر زمـان رایانه جدیدی را تحـت تأثیر قرار می داد. کرمها و ویروسـها از دو طریق منتقل می شوند:

(۱) با دیسـکت : اولین راه از طریق یک دیسـکت تحت تأثیر قرار گرفته است. شاید از یک دوست یا یک فرد تعمیر کار رایانه گرفته شـده باشد. (۲) با شبکه: راه دوم از طریق یک شـبکه اسـت مانند گرفتن ویروس از پسـت الکترونیکی یا یک تابلـوی اعلانات الکترونیکی. این همان دلیلی است که هنگامی که از مزیت های همهٔ

بـازی های آزاد یـا دیگر نرم افزارهایـی که به صورت پیوسـته در دسترس است، اسـتفاده می کنید باید از نرم افزار و ویروس یاب استفاده شود تا فایل های بارگذاری شده را اسکن کند.

● ویروس معمولاً به دیسـک سـخت رایانه یا تلفن همراه پیوست می شود. ممکن است بعداً پیامهای ناراحت کننده‌ای مانند «این رایانه تبدیل به سـنگ می شود!» و ... ارسال می کند یا موجب ایجاد توپهای پینگ پونگی شود که در اطراف صفحه نمایش شما بالا و پایین می روند و متن را مورد ضربه های خود قرار دهند و در آن اشکال ایجـادکننـد.

در مراحـل جدی و پیشـرفته تر به فایـل های متنی چیزهـای به درد نخور و نامربـوط اضافه کند و حتی نرم افزار سیستمی را پاک کند یا از کار بیندازد. این ویروس ها از اینکه بتوان با جسـتجو آن را یافت، ممکن است خود را پنهان کند و خسارتش را به جاهای دیگر نیز گسترش دهد، زیرا دیسـک سـخت از هر فلاپی دیسـکی که به وسیلهٔ سـامانه به کار رود تأثیر می پذیرد. اگر به انباره[۸] هـر نرم افزار نظری بیندازیم تنوع زیادی در برنامه های ضـد ویروس خواهیم دید. نـرم افزارهای ضد ویروس دیسک سـخت رایانه، فلاپی دیسکها و حافظهٔ اصلی را اسـکن می کنند تا ویروسها را بیابند و گاهاً آنها را نابود می کنند. این پاسـدارهای رایانه ها بـه دو طریق عمل می کنند. اول این که دیسـک گـردان ها را برای علائم و امضاهـا اسـکن می کنند. زنجیرهٔ ویـژه ای از صفر و یـک ها در ویروس که به طور بی نظیری وجود دارد را تشـخیص می دهد. دوم آن که رفتارهای شبه ویروسی مشـکوک را اسـکن کرده و می یابند مانند تلاش برای پاک کردن یـا تغییر دادن مکان فایلها روی دیسـکهای رایانه. چند نرم افزار ضدویـروس که پرکاربردتر بوده، نورتون آنتی ویروس ۲۰۰۰، ویروس اسکن McAfee جهـت نصب روی ویندوز و Virex جهت نصب روی مکینتاش می باشد.

● به طور کلی خطاها و سوانح می‌تواند در سامانه‌های رایانه ای به (۱)خطاهای انسـانی، (۲)خطاهای روشـی یا عملکـردی، (۳)خطاهای نرم افزاری، (٤)مشـکلات الکترومکانیکی و (۵)مسـائل پدید آمـده از دادهٔ آلوده دسته بندی شود (Sawyer, 2001).

– خطاهـای انسـانی را غالباً کارشناسـان در مورد تأثیرات ناخواسـتهٔ فناوری صحبت می کنند آنچه بدان اشـاره می کنند موارد غیرمنتظره ای اسـت که افراد با آن فناوری انجام می دهند. مواردی که افراد می توانند مسائل یک سـامانه را وخیم تر و حادتر کنند به این قرار است: (۱) افراد غالباً در ارزیابی نیازهای اطلاعاتی شان به نحو احسن عمل نمی کنند. برای مثال، خیلی از کاربران رایانه و سیسـتمهای ارتباطی که چندان پیچیده و به حد کافی پیشـرفته نیسـتند را به کار می برند، عـده ای نیز خیلی پیچیده تر از حد نیاز آنهاست. (۲) عواطف و احساسات انسـانی روی اجرای او تأثیر مـی گذارد. برای مثال یک تجربـهٔ عـذاب آور با یک رایانه کافی اسـت تا افراد را مجبور کند کل سـامانه را ترک و تسـلیم شوند. اما این عکس العملها نمی تواند این امکان را بدهد تا اینکه بهتر و بیشتر یاد بگیریم که چطور از آن سامانه استفاده کنیم. (۳) افراد بر مبنای اسـتنباط شـان عمل می کنند که در محیط های اطلاعاتی مدرن غالباً خیلی آرام هسـتند تا با تجهیزات کارشـان را ادامه دهند. تصمیمات تحت تأثیر اطلاعاتـی که گرد آمده، اتخاذ می گردند. به عنوان مثال به همان اندازه دارای خطا می تواند باشـد که بر اساس اطلاعات خیلی کم اتخاذ شده باشد.

– خطاهای روشی مربوط به طرز عمل و عملکرد. بعضی از اعمـال ناموفق رایانه ای غیرقابل باور اتفاق افتاده چرا که بعضی از افراد روال کار را درست دنبال نکرده اند .

در سال ۱۹۹۹، پروژه ۱۲۵ میلیون دلاری مارس کلایمت اربیتر داده‌ای که به آن داده می شـد را به پوند نشان می داد، واحد انگلیسی نیرو، به جای نیوتون (حدود ۲۲ درصد یک پوند) است، در نتیجه فضاپیمای مریخ خیلی نزدیک به سطح مریخ شد و در اثر اصابت از هم متلاشی شد.

چند سـال قبل در دومین بازار بزرگ بورس، نسدق، حدود ۲/۵ ساعت عملکردش متوقف شد و عجیب آنکه برای آن تلاش داشـتند سـامانه رایانه ای را برای کاربران راحت‌تر و ساده‌تر کنند. متخصصین فنی مرحله به مرحله نرم افزار جدید را اجرا کردند و پیشرفتهای فنی را در یک روز و یـک زمان اضافه و اجرا کردنـد. چند روز به این فرایند مانده، تکنسین ها تلاش می کردند که ویژگی های بیشـتری به نرم افزار آن اضاف کننـد تا از قدرت ذخیره اطلاعات زیادی ، سامانه رایانه ای برخوردار گردد. نتیجه به تأخیر انداختن سـاعت گشـایش بازار بورس و کوتاه شدن روز خرید و فروش سهام در بازار بود.

– خطاهای نـرم افـزاری. امروزه همـواره از نقص یا اشکالات نرم افزاری سخن گفته می شود. اشکال نرم افزاری یک خطاسـت کـه در برنامه ایجاد می شـود و موجب درسـت کار نکردن آن می شود. در یک ستون روزنامه که اظهار تأسف می شد از عدم حضور یک مرورگر وب بـی عیب و نقص، روزنامه نگار بیزینس ویک، «اسـتفن وایلد اسـتروم» این طور نوشت: من هر مرورگری را که نت اسـکیپ تولید کرده اسـتفاده کـرده ام و همه آنها

دارای مشـکل و معیوب اند. اما رقیب اصلی آن نیز بهتر نیست». جایی که نت اسـکیپ در سراشیبی سقوط بود وایلد اسـتروم چنیـن اظهار می کـرد: مرورگر IE7/0 مایکروسافت تصویر ترسـناکی از خود به وجود آورده اسـت . به وصله های[9] نرم افزاری زیادی نیاز اسـت تا منافذ و سـوراخ‌های امنیتی موجود در نـرم افزار را که به بیگانگان اجازه می دهد به رایانه ها دسترسـی یابند، ببندد.

– اشـکالات الکترومکانیکی. سامانه های مکانیکی نظیر چاپگرها و سامانه های برقی مانند صفحات مدارها همیشـه درسـت کار نمی کنند. ممکن اسـت اشـتباهاً سـاختاربندی یا کثیف شـده باشـند یا زیاد از حد گرم شـده باشند، سیمها جدا باشند یا از طریق راه های دیگر به آنها آسـیب رسیده باشـد. قطع و وصل تغذیه برق (قهوه ای یا مشـکی) مـی تواند یک سـامانه را از کار بینـدازد همچنین نارسـایی های تغذیه بـرق می تواند تجهیزات را بسوزاند.

– سـامانه های مدرن از هزارها جزء سـاخته شده اند، همهٔ آنها به هم مربوط هسـتند بـه نحوی که پیش بینی آن غیرممکن اسـت. به خاطر پیچیدگی، جامعه شـناس دانشـگاه ییل، چارلـز پرو، اینطور بحـث می کند آنچه اتفاقـات و سـوانح طبیعی قلمـداد می شـود غیرقابل اجتناب اسـت. به همین دلیل، این تقریباً مسلم است که ترکیب عدم موفقیت های جزئی سـرانجام جمع شده و منجـر به چیزی مثل فاجعه می گردد. در واقع، این فقط مجموعه هایـی نظیر آن ناکامی‌های کوچکی اسـت که منجر به حوادثی نظیر منفجر شدن فضاپیمای چلنجر در سال ۱۹۸٦ و حالت بحران گداخت و فروپاشی در هستهٔ مرکزی در جزیرهٔ سـه مایلی رآکتور هسته ای آمریکا در سـال ۱۹۷۹ اسـت. در عصر دیجیتال اتفاقات طبیعی نه تنها چیـز غیرعادی و خلاف قاعـده نخواهد بود بلکه انتظار هم می رود.

– مسـائل مربوط به دادهٔ آلـوده. وقتی که یک مقاله تایپ می شود بی شک تعداد معدودی غلط تایپی وجود خواهد داشت که امید می رود آنها پاک و برطرف شوند؛ همانطور نیز همهٔ افرادی که در سراسر دنیا داده وارد می کنند و کسـانی که یک زنجیرهٔ ممتد از داده را به سامانه های رایانه ای وارد می کنند، بسـیاری از مسـائل از این قبیل از طریق همین داده ی آلوده پدید می آید. داده آلوده یا کامل نیسـت یا از تاریخ آن گذشته یا از طرف دیگر آن داده دقیق نیست. یک دلیل خوب برای یک نظر انداختن به رکوردهای اطلاعات دارد – اعم از اعتباری، پزشکی، آموزشـی – این است که می توان هر تصحیحی را روی آنها قبل از اینکه مسائل و مشکلاتی را برای کل سامانه به بار آورند، انجام داد. همانطور که مدیر یک شـرکت کاملاً تخصصی در هوش تجاری چنین می نویسد: پایگاه های داده الکترونیک هنگامـی که یک منبع ذخیرهٔ زمان برای جویندهٔ اطلاعات باشـد، همانطور نیز می تواند به عنوان کاتالیست به بزرگ جلوه دادن و سرعت بخشیدن به داده نادرست و آلوده کمک کند.

● بلایای طبیعی و دیگر سـوانح. برخی از سـوانح صرفاً منجر به تعطیلی موقت سامانه نمی شوند، بلکه می توانند کل سـامانه را نابود کنند. برای مثـال هایی از این قبیل می توان به سـوانح طبیعی ، کشـمکش هـای داخلی و تروریسم اشاره کرد.

– سوانح طبیعی. هر چه که زیان آور است برای مال و جان افراد برای رایانه و سـامانه های ارتباطی نیز زیان آور است که شامل بلایای طبیعی مانند آتش سوزی ها ، سیلها و ویرانگـری هـای آن، زلزله ها، طوفانهـا و تندبادها و مانند آن اسـت. سـوانح طبیعی روی یک ناحیهٔ گسترده نظیـر طوفانهای یـخ و برف در شـرقی تریـن نواحی کانادا یا تندبادهای فلوریدا، می تواند همهٔ سـامانه‌های الکترونیکی که خیلـی خوب و بی نقص به کار انداخته بودیـم را از کار بیندازد. بدون انـرژی برق و اتصالات ارتباطی، ماشینهای ATM ، تأییدکنندهٔ کارتهای اعتباری و رایانه های بانک غیرقابل استفاده هستند.

– کشـمکش هـای داخلـی و تروریسـم. ممکن اسـت خیال راحتی داشته باشـیم که جنگها و شورشها در قسـمتهای دیگر دنیـا اتفاق می افتـد و به منطقه ما راه نـدارد اما تضمینی وجود نـدارد و البته همچنان نیز در مقابل آشـوبهای داخلی مانند هیجـان خواهی های طرفداران تیمهای ورزشی مصون نیستیم ، نظیر بلواهایی که در لوس آنجلس آمریکا در سـال ۲۰۰۰ پس از اینکه تیم لیکرز در خانهٔ خود قهرمانی NBA را کسـب کرد، اتفاق افتاد. ما آشـکارا در مقابل اعمال تروریستی ایمن نیستیم.

نظیر بمب گذاری سال ۱۹۹۳ و سال ۲۰۰۱ در مرکز تجـارت جهانی و حملهٔ هواپیماها به برج های دوقلوی شهر نیویورک.

در این موارد بود که شـرکتها دریافتند که شتابزده تجهیزات خود را به ادارات جدید منتقل کنند و شـبکه های رایانه ای شـان را دوباره تأسـیس کننـد. پنتاگون (وزارت دفاع آمریکا) که ٦۵۰۰۰۰ پایانه و ایستگاه کاری ، ۱۰۰ شـبکه گسـترده WAN و ۱۰۰۰۰ شبکهٔ محلی LAN دارد، قدمهایی را در جهت کاهش آسیب پذیری سامانه هایش دربرابر متجاوزان برداشته است.

علی رغم اینکه نفوذگران اقدام به نفوذ در عملیات های فوق سرّی می کنند. (ویلیامز، استیسی، ۲۰۰۱)

● رمز نگاری[۱۰] پل کوشـر رئیس و برجسـته ترین دانشـمند مرکز تحقیقات رمزنگاری اعلام داشت که در طول ۲۰ سال گذشته ، اغلب اقداماتی که در زمینهٔ امنیت رایانه ها صورت گرفته بر ایجاد سـامانه هایی قدرتمند در برابر حملات تمرکز داشته است. این پرسش که پس از بروز اشـکال در سیسـتم چه خواهید کـرد، منجر به ایجاد سیسـتمهای موفقی گردیده اسـت، اما در اغلب موارد تحقیقات اندکی صورت گرفته و ساختار زیربنایی ناچیزی به آنها اختصاص یافته است.به عنوان مثال اگر نرم افزار ویروس یاب را بررسـی کنید، درخواهید یافت که از یک روش واکنشی در آن استفاده شده است. هنگامی که به مقولهٔ محافظت در برابر سـرقت فیلم، موسیقی و یـا بازی ها برمی خوریم، این عقیده وجود دارد که باید جعبـه ای قدرتمنـد ایجاد کرده و ابـزار لازم را در آن قرار دهید و امیدوار باشـید که این جعبه هیچ گاه دچار مشکل نمی شـود. اما این مدل غیرواقعی است؛ چرا که شما نمی توانید سیستمهای پیچیده و ارزان قیمتی ایجاد کنید که توسط مهندسـان ناآگاه از مسائل امنیتی توسعه یافته باشند. (ماهنامه وب، ۱۳۸۵)

مهمترین گرایش‌ها در زمینه رمزنگاری و امنیت IT در ده سـال آینده مقابله با حملات هدفمند است. یکی از تهدیدات بالقوه همین حملات هدفمند است مانند آن که شـخصی بخواهد نامه های الکترونیکی تجاری شما را بخوانـد تا از آن سوءاسـتفاده کند. اغلب محصولات به گونه ای طراحی می شـوند کـه در تمامی اوقات از تمامـی کاربران محافظت کنند ولـی به منظور محافظت از موقعیتـی که در آن شـخص خاصی مورد هدف قرار گرفته باشـد یا حمله از پیش طراحی شـده ای صورت گیرد، پیش بینی نمی شوند.

اگـر بتوانید ۹۹/۹ درصد از رایانه های شـبکه خود را از ویـروس دور نگه دارید، کار بزرگی در زمینهٔ رفع معضـل ویروس ها انجام داده اید؛ اما در صورتی که آن ۰/۱ درصد باقی مانده، مربوط به اطلاعات حساس شما باشد، در واقع هیچ کار مهمی انجام نداده اید.

پی نوشت

۱ – فناوری های های–تک معطوف به فناوری های برتر چون ساخت روباتها و هوش مصنوعی می باشد.
۲ – آلوین تافلر
۳ – User interfaces
٤– multi media resources center(مرکز منابع چندرسانه ای)
٥– Cracker فردی که از معیارهای امنیتی در سیستم رایانه ای عبور کرده و دسترسی غیرمجازی را برقرار می کند. غالباً هدف این افراد کسب غیرقانونی اطلاعات از سیستم رایانه ای یا استفاده از منابع آن سیستم است.
٦– علمی که خصوصیات بدنی هر فرد را اندازه گیری می نماید.
۷- phone phreaks
۸ - utility
۹- PATCH
۱۰- cryptography

منابع وماخذ

۱. آرمز ، ویلیام (۱۳۸۱) ، **کتابخانه های دیجیتالی** ،ترجمه زهیر حیاتی، هاجر ستوده، تهران، چاپار.
۲. آزاد، اسداله(۱۳۷٤). **کتابداری و اطلاع رسانی در عصر حاضر**. فصلنامه کتاب ،دوره ٦ ، شماره ۳ و ٤
۳. احمدی لاری ،رکن الدین، فرزین، فرزانه(۱۳۷۵) ، **آموزش کتابداری و اطلاع رسانی در عصر فناوری** ،مجله علوم اجتماعی و انسانی دانشگاه شیراز ،شماره اول
٤. ایمانی‌کیا، حمیدرضا. **نگرشی بر اهداف و برنامه های ابر بزرگراه های اطلاعاتی (درآمریکا)**. رایانه: ٥٤.
٥. تل، بجورن (۱۳٦۱). **تحول نقش متخصصان کتابخانه ها و مراکز اطلاع رسانی**. ترجمه سعیده ذکریا، نشریه

مرکز اطلاعات و مدارک علمی ایران ،دوره ششم ، شماره۱و۲ .
٦. حیاتی ، زهیر(۱۳۸۰)**کتابداران در چالش یا فناوریهای اطلاعاتی** ،رهیافت،شماره ۲۵ .
۷. حیاتی ،زهیر(۱۳۷۸) « **استفاده از اینترنت در آموزش** «. اینترنت ، جنبه های نظری و کاربردی آن ، به کوشش حمید محسنی ، تهران ، نشرکتابدار.
۸. **رمز نگاری**. ماهنامه وب ۷(۷٦). ۱۳۸۵.
۹. داورپناه ،محمدرضا(۱۳۷۸). **برنامه ریزی زیر ساخت فناوری اطلاعات در کشورهای در حال توسعه** ، کتابداری و اطلاع رسانی ،سال ۲ ، شماره ۳ .
۱۰. زوارقی ،رسول (۱۳۸۳).**تحولات فناوری کتابخانه ها**، مجله الکترونیکی مرکزاطلاعات و مدارک علمی ، ۲(۲).
۱۱. **سرعت بالا وسعت زیاد: اینترنت II دیوانه وار در راه است**. ترجمه محمد ناصح. ماهنامه وب ٦(٦٤). ۱۳۸٤
۱۲. علی اکبرزاده ، هیلان،(۱۳۷۷)،کتابداران در قرن بیست و یکم ،فصلنامه کتاب .
۱۳. کیوان، کوشا (۱۳۷۹). **فهرست همگانی و شبکه جهانی وب : بررسی امکانات فهرست پیوسته کتابخانه ها** در محیط وب ، مرکز اطلاع رسانی و خدمات علمی جهاد کشاورزی.
۱٤. **گوگل بزرگ ترین کتابدار دیجیتالی جهان می شود**. ماهنامه وب ٦(٦٤). ۱۳۸٤.
۱۵. **کره ای ها مقام سوم دنیای مجازی شدند**. ماهنامه وب ٦(٦٤). ۱۳۸٤.
۱٦. ویتور،رولاند (۱۳۸۳). **کتابخانه های تخصصی :چگونگی حیات در قرن بیست و یکم** ، ترجمه جواد بشیری ، پیام کتابخانه ،۱۲(۳،٤).
۱۷. یاری فیروزآبادی، یارحسین (۱۳۸۵). **کتابخانه های تخصصی و فناوری اطلاعات** . مجله الکترونیکی پژوهشگاه اطلاعات و مدارک علمی ، دوره ۳ شماره ٦ .

Abdullahi, Ismail, **« educating the information professional for the twenty firs century»**. the 1st china – united states library conference. [Online] available at: http://darkwing.uoregon.edu/~felsing/ala/abdullhi.html [accessed 23 December 2008]

Horn, j (2000). **The future is now: reference service for the electronic era**. Reference review, 4(6). p. 32-42.

Johnston, Colin (1998).**« Electronic technology and its impact on libraries »**. Journal of librarianship and information science, 30(1). pp 7-24. [online] available at: http://lis.sagepub.com/cgi/content/abstract/30/1/7 [accessed 1 January 2009]

King, R. James (2004), **the Future of the special library: one person's perspective**. Library Science and Technology, 30(3). pp. 171-175. [Online] available at: http://sciencedirect.com [accessed 2 July 2008]

Library of Congress,(1999). **Reference service in a digital age**. [Online] available at: http://www.lcweb.loc.gov/vv/digivef/ [accessed 25 September 2008]

Mayo M. Lesley (2002). Reference any time any where: towards virtual reference services at penn state. The Electronic Library, 20(1).

Philip, B.(1999). **May I help you @ the electronic reference desk.: an examination of the past , present and future of electronic mail reference service** . [Online] available at: http://hollyhock.slis.valberta.ca/598/brenda/emailref.htm [accessed 20 November 2008]

Sabaratnam, Julies, (1997).**« Planning the library of the future: the Singapore experience».** IFLA Journal, no 3 , pp.197-202

Williams, Brian K. Sawyer, Stacey C. (2001). **"the challenges of the digital age"**, Using Information Technology. Mc Graw Hill.