نقش مدیران و کاربران در سیستم‌های اطلاعاتی: چالش‌ها و تهدیدها

سید حسن صادق زاده[۱]، محسن غلام زاده[۲]

[۱] مربی، گروه کامپیوتر و فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه پیام نورج.ا. ایران(مدرس دانشگاه علمی کاربردی بشرویه)

Sadeghzadeh@pnu.ac.ir

[۲] دانشجوی کارشناسی، گروه کامپیوتر، دانشگاه پیام نور استان یزد-طبس، ایران

Sharif.pnu@gmail.com

چکیده

شرایط جنگ و دفاع در عصر سایبر چنان متحول شده است که ما نیازمند طیف جدیدی از مدیران و کاربران دفاعی آشنا با مسائل امنیتی و مسلط به استفاده از سیستم‌های اطلاعاتی هستیم. اصول نوین حاکم بر فضای سایبر، ما را ملزم به شناخت فضای جدید و استفاده مناسب از دانش و ابزارهای روز می‌نماید تا بتوان مسائل امنیتی را بهتر بکار برد. بی شک مدیران و کاربران سیستم‌های اطلاعاتی بیشترین نقش را در مسائل نامبرده دارند زیرا عدم دقت و تجربه کافی این افراد می‌تواند صدمات جبران ناپذیری را وارد کند. بنابراین در این مقاله بعد از معرفی انواع سیستم‌های اطلاعاتی به نقش مدیران و کاربران در سیستم‌های اطلاعاتی پرداخته، چالش‌ها و تهدیدهایی که می‌تواند توسط این افراد انجام شود را بیان می‌کنیم.

واژگان کلیدی:

جنگ اطلاعات، سیستم های اطلاعاتی، امنیت، مدیران و کاربران سیستم

۱- مقدمه

بیش از هشتاد درصد کار روزانه مدیران صرف اطلاعات می‌شود از جمله دریافت اطلاعات، برقراری ارتباط و استفاده از اطلاعات در طیف وسیعی از امور مختلف. از آنجایی که اطلاعات مبنای تمام فعالیت‌های یک سازمان است، سیستم‌هایی باید وجود داشته باشند که اطلاعات را تولید و مدیریت کنند. هدف چنین سیستم‌هایی ایجاد تضمین در ارائه اطلاعات صحیح و قابل اطمینان در مواقع مورد نیاز و در شکل قابل استفاده است. چنین سیستم‌هایی، سیستم‌های اطلاعات نامگذاری شده‌اند. استفاده از چنین سیستم‌هایی بدون استفاده از مدیران و کاربران خبره امکان پذیر نخواهد بود و عدم دقت و تجربه کافی این افراد می‌تواند صدمات جبران ناپذیری را وارد کند. بنابراین هدف این مقاله بررسی چالش‌ها و تهدیدهایی است که می‌تواند توسط این افراد انجام شود و سیستم را دچار مشکل سازد. امید است با رعایت مسائل معرفی شده بتوان سیستم‌های اطلاعاتی امن و مطمئن‌تری داشته باشیم.

۲- سیستم های اطلاعاتی

سیستم اطلاعات عبارت است از یک سیستم کامل طراحی شده برای تولید، جمع آوری، سازماندهی، ذخیره، بازیابی و اشاعه در یک موسسه، سازمان یا هر حوزه تعریف شده دیگر از جامعه. امروزه بهره گیری از سیستم‌های اطلاعاتی در حیطه موضوعات سازمانی که در گذشته تنها با نبوغ و قضاوت انسان قابل حل بود، افزایش یافته است[۱]. سیستم‌های اطلاعاتی صرفا ابزاری برای تصمیم گیری هستند، اما باید دانست که هر یک از این سیستم‌ها هم تصمیم گیری و هم فراهم کردن بستر تخصصی و حرفه ای ارتباطات کاری در سازمان را پشتیبانی می‌کنند. برای روشن تر شدن این مفهوم و آگاهی از نحوه اثر این سیستم‌ها روی فرآیندهای ارتباط و تصمیم-گیری در سازمانها، به توصیف مختصر هر یک از سیستم‌های اطلاعاتی می‌پردازیم:[۲]

۲-۱- سیستم‌های اطلاعاتی اتوماسیون اداری (OAS)

جمع آوری و نگهداری اطلاعات در ارتباط با عملیات سازمان و کنترل برخی ویژگی‌های عملیاتی در سازمان از طریق فرمت‌های ویژه و مشخصات اطلاعات؛

- کاربران سیستم: هر کس که داده‌های شخصی را نگهداری می‌کند، اسناد را تهیه می‌کند، یا محاسبه انجام می‌دهد.
- اثر روی ارتباطات: از طریق ابزار ایجاد اسناد و ارائه اسناد و مدارک، از قبیل واژه پردازها، و نرم افزارهای نمایش اسلاید مانند(Power Point)
- اثر روی تصمیم‌گیری: از طریق کاربرگ‌های الکترونیکی مانند(Excel) و دیگر نرم افزارهای تجزیه و تحلیل اطلاعات.

۲-۲- سیستم‌های اطلاعاتی ارتباطات الکترونیکی (ECS)

برای انجام کارهای گروهی و ارتباط با یکدیگر از طریق تبادل و انتشار اطلاعات در فرم‌های مختلف به پرسنل کمک می‌کند؛

- کاربران سیستم: هر کس؛ اعم از کارکنان، مدیران، یا دیگران خارج از سازمان، که بخواهد ارتباط برقرار کنند.
- اثر روی ارتباطات: از طریق تلفن، کنفرانس‌های ویدئویی، پست الکترونیک، فاکس، دسترسی به اطلاعات مشترک، جلسات غیر حضوری یا مجازی، کنترل جریان کارها.
- اثر روی تصمیم گیری: از طریق تلفن و کنفرانس‌های راه دور برای تصمیم گیری پست الکترونیکی یا فاکس و امثال آن‌ها برای دریافت اطلاعات پشتیبانی اطلاعات مشترک برای اتخاذ تصمیمات جمعی و هماهنگ.

۲-۳- سیستم‌های اطلاعاتی عملیاتی(TPS)

جمع آوری و نگهداری اطلاعات در ارتباط با عملیات سازمان و کنترل برخی ویژگی‌های عملیاتی در سازمان از طریق فرمتهای ویژه و مشخصات اطلاعات؛

- کاربران سیستم: کارکنانی که کار آن‌ها در ارتباط با فعالیت‌های سازمانی است.
- اثر روی ارتباطات: با ایجاد بانک‌های اطلاعاتی که می‌توانند به طور مستقیم در دسترس قرار گیرند، و برخی ارتباطات رو در رو بین پرسنل را پشتیبانی می‌کنند.
- اثر روی تصمیم گیری: در جریان نگهداری اطلاعات عملکرد سازمان، بازخورد فوری ارائه می‌کند و روی تصمیمات اتخاذ

شده بر اساس این اطلاعات اثر می‌گذارند؛ اطلاعات مفید برای برنامه ریزی و تصمیم گیری مدیران ارائه می‌کنند.

۲-۴- سیستم‌های اطلاعاتی مدیریت(MIS) و (EIS)

داده‌های سیستم هایTPSرا برای نظارت بر عملکرد سازمان در اختیار مدیران قرار می‌دهند؛

- ❖ کاربران سیستم: مدیران، سرپرستان و کارشناسانی که به بازخورد کار خود نیاز دارند.
- ❖ اثر روی ارتباطات: واقعیت‌های کاری و عملکرد سازمان را برای تشریح مشکلات و راه حل‌های آن‌ها ارائه می‌کنند و ممکن است با پست الکترونیکی و دیگر روش‌های ارتباط برای ارائه داده‌ها به صورت دیجیتالی ترکیب شوند.
- ❖ اثر روی تصمیم گیری : خلاصه اطلاعات و کمیت عملکردها را برای مشاهده و نظارت بر نتایج عملکردها ارائه می‌کنند و ممکن است راه‌های ساده تری برای تجزیه تحلیل انواع اطلاعاتی که قبلادر فرم‌های ثابت ویکنواختMIS ارائه می‌شد ارائه کنند.

۲-۵-سیستم‌های اطلاعاتی پشتیبان تصمیم گیری (DSS)

با ارائه اطلاعات، مدل ها، یا ابزار تجزیه و تحلیل به اتخاذ تصمیم‌ها در سازمان کمک می‌کنند؛

- ❖ کاربران سیستم: تحلیل گران، مدیران و دیگر متخصصین سازمان.
- ❖ اثر روی ارتباطات: تجزیه و تحلیل با استفاده از این سیستم‌ها موجب ارائه شفاف و گویای اطلاعات و مشکلات برای کمک به تصمیم گیری خواهد شد.
- ❖ اثر روی تصمیم گیری: از طریق ارائه ابزاری برای تجزیه تحلیل و مدلسازی داده‌ها از طریق تعریف و ارزیابی راه حل ها.

۲-۶-سیستم‌های اطلاعاتی سازمانی: جامع و یکپارچه(ES)

ایجاد و حفظ یکپارچگی روش‌های پردازش داده‌ها و تامین یک بانک اطلاعاتی یکپارچه و پیوسته مرکزی برای ارتباط با تمام حوزه‌ها و سیستم‌های اطلاعاتی سازمان؛

- ❖ کاربران سیستم: افرادی که اطلاعات اجرای فرآیندها را وارد می‌کنند، مدیران، سرپرستان و هر کس که به اطلاعات اجرای فرآیندها نیاز دارد.
- ❖ اثر روی ارتباطات: از طریق نگهداری بانک اطلاعاتی که می‌توان به طور مستقیم به آن دسترسی داشت، برخی ارتباطات رو در رو بین پرسنل و مدیران را برقرار می‌کند. از طریق ایجاد و حفظ یکنواختی در گردش اطلاعات موجب تسهیل ارتباطات می‌شود.
- ❖ اثر روی تصمیم گیری: از طریق یک بانک اطلاعاتی ویژه، اطلاعات یکنواخت و پیوسته برای کمک به تصمیم گیری ارائه می‌کند. از طریق ایجاد و حفظ یکنواختی در گردش اطلاعات موجب تسهیل استفاده از اطلاعات در جریان تصمیم گیری‌ها می‌شود.[۸و۷]

۳- تدابیر مدیریتی

کنترل‌های مدیریتی غالبا به برقراری کنترل‌ها از طریق دستورالعمل‌ها و روش‌ها تاکید دارد مانند انتخاب صحیح کارکنان، آموزش و پرورش و سرپرستی آن‌ها در حیطه سیستم‌های اطلاعات. برخی از اقدامات عبارتند از:

- ممانعت از دسترسی کارکنانی که اخراج، بازنشسته و یا انتقال می‌یابند.
- تدوین و تهیه استانداردهای توسعه سیستم‌ها و مستندات آن
- انجام بازرسیهای مستمر از سیستم‌ها (برنامه ای و دارای زمان بندی)

مدیران شبکه (سیستم)، مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می‌باشند که حرکت و یا حرکات اشتباه هر یک می‌تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را بدنبال داشته باشد. در ادامه به بررسی اشتباهات متداولی خواهیم پرداخت که می‌تواند توسط سه گروه یاد شده انجام و زمینه بروز یک مشکل امنیتی در رابطه با اطلاعات حساس در یک سازمان را باعث گردد.

۳-۱- اشتباهات متداول مدیران سیستم

مدیران سیستم ، به افرادی اطلاق می‌گردد که مسئولیت نگهداری و نظارت بر عملکرد صحیح و عملیاتی سیستم‌ها و شبکه موجود در یک سازمان را برعهده دارند . در اغلب سازمان‌ها افراد فوق، مسئولیت امنیت دستگاه ها، ایمن سازی شبکه و تشخیص ضعف‌های امنیتی موجود در رابطه با اطلاعات حساس را نیز برعهده دارند در ادامه با برخی از

خطاهای متداولی که ممکن است توسط مدیران سیستم انجام و سازمان مربوطه را با تهدید امنیتی مواجه سازد، آشنا خواهیم شد.[۴و۳]

۳-۱-۱- عدم وجود یک سیاست امنیتی مشخص

اکثر قریب به اتفاق مدیران سیستم دارای یک سیاست امنیتی مشخص بمنظور انجام فعالیت‌های مهمی نظیر امنیت فیزیکی سیستم ها، و روش‌های بهنگام سازی یک نرم افزار در زمان مربوطه نمی باشند. در برخی حالات، مدیران سیستم حتی نسبت به آخرین نقاط آسیب پذیر تشخیص داده شده نیز آگاهی به هنگامی نداشته بااین وجود نقاط آسیب پذیر در شبکه می‌تواند یک سازمان را در معرض تهدیدات جدی قرار دهد.[۵و۳]

۳-۱-۲- اتصال سیستم‌های فاقد پیکربندی مناسب به اینترنت

همزمان با گسترش نیازهای سازمان، سیستم‌ها و سرویس دهندگان جدیدی بر اساس یک روال معمول به اینترنت متصل می‌گردند. اکثر اینچنین سیستمهائی بدون تنظیمات امنیتی خاص به اینترنت متصل شده و می‌تواند زمینه بروز آسیب و حملات اطلاعاتی توسط مهاجمان را باعث گردد.

به هرحال همواره ممکن است افرادی بصورت مخفیانه شبکه سازمان شما را پویش کنند تا در صورت وجود یک نقطه آسیب پذیر، از آن برای اهداف خود استفاده نمایند. لازم است در این راستا تهدیدات و خطرات را جدی گرفته و پیگیری لازم در این خصوص انجام شود.[۵و۴]

۳-۱-۳- اعتماد بیش از اندازه به ابزار ها

برنامه‌های پویش و بررسی نقاط آسیب پذیر، اغلب بمنظور اخذ اطلاعات در رابطه وضعیت جاری امنیتی شبکه استفاده می‌گردد. در این رابطه لازم است متناسب با نوع سیستم عامل نصب شده بر روی سیستمها از پویشگران متعدد و مختص سیستم عامل مربوطه استفاده گردد. به هرحال استفاده از این نوع نرم افزارها قطعاً باعث شناسائی سریع نقاط آسیب پذیر و صرفه جوئی زمان می‌گردد ولی نباید این تصور وجود داشته باشد که استفاده از آنان بمنزله یک راه حل جامع امنیتی است. تاکید صرف بر نتایج بدست آمده توسط آنان، می‌تواند نتایج نامطلوب امنیتی را بدنبال داشته باشد.[۵و۳]

۳-۱-۴- عدم مشاهده گزارش‌ها (Logs)

مشاهده گزارش‌های سیستم، یکی از مراحل ضروری در تشخیص مستمر و یا قریب الوقوع تهدیدات است. گزارش ها، امکان شناسائی نقاط آسیب پذیر متداول و حملات مربوطه را فراهم می‌نمایند. بنابراین می‌توان تمامی سیستم را بررسی و آن را در مقابل حملات مشخص شده، مجهز و ایمن نمود. در صورت بروز یک تهاجم، با استفاده از گزارش‌های سیستم، تسهیلات لازم بمنظور ردیابی مهاجمان فراهم می‌گردد.

۳-۱-۵- اجرای سرویسها و یا اسکریپت‌های اضافه و غیرضروری

استفاده از منابع و شبکه سازمان، بعنوان یک زمین بازی شخصی برای تست اسکریپت‌ها و سرویس‌های متفاوت، یکی دیگر از اشتباهات متداولی است که توسط اکثریت قریب به اتفاق مدیران سیستم انجام می‌شود. داشتن اینچنین اسکریپت‌ها و سرویس‌های اضافه ای که بر روی سیستم اجراء می‌گردند، باعث ایجاد مجموعه ای از پتانسیل‌ها و نقاط ورود جدید برای یک مهاجم می‌گردد در صورت نیاز به تست اسکریپت‌ها و یا اجرای سرویس‌های اضافه، می‌بایست عملیات مورد نظر خود را از طریق یک کامپیوتر ایزوله شده انجام داد.

۳-۲- اشتباهات متداول مدیران سازمان ها

مدیران سازمان، به افرادی اطلاق می‌گردد که مسئولیت مدیریت، هدایت و توسعه سازمان را بر عهده داشته و با منابع متفاوت موجود در سازمان نظیر بودجه، سروکار دارند. در صورتیکه سازمان‌ها و موسسات دارای یک استراتژی امنیتی مشخص شده ای نباشند، اتصال به شبکه جهانی تهدیدی در ارتباط با اطلاعات حساس خواهد بود. در ادامه به برخی از اشتباهات متداول که از ناحیه مدیران سازمان بروز و تاثیر

منفی در ارتباط با امنیت اطلاعات در سازمان را بدنبال خواهد داشت، اشاره می‌گردد:

۳-۲-۱- استخدام کارشناسان آموزش ندیده و غیرخبره

بدون تردید، کارشناسان آموزش دیده و خبره، یکی از منابع ارزشمند در هر سازمان محسوب می‌گردند. همواره می‌بایست از کارشناسان ورزیده در ارتباط با امنیت در یک سازمان استفاده گردد. امنیت اطلاعات از جمله مقولاتی است که برای یک سازمان دارای جایگاهی است و همواره می‌بایست بهترین تصمیم دررابطه با استفاده از منابع انسانی ماهر، اتخاذ گردد. استفاده از یک کارشناس غیر ماهر در امور امنیت اطلاعات و شبکه در یک سازمان، خود تهدیدی امنیتی است که بر سایر تهدیدات موجود اضافه خواهد شد.

۳-۲-۲- فقدان آگاهی لازم در رابطه با تاثیر یک ضعف امنیتی بر عملکرد سازمان

بسیاری از مدیران سازمان همواره بر این باور می‌باشند که "این مسئله برای ما اتفاق نخواهد افتاد" و بر همین اساس و طرز فکر به مقوله امنیت نگاه می‌نمایند. این مسئله می‌تواند بدلیل عدم آشنائی با ابعاد و اثرات یک ضعف امنیتی در سازمان باشد. بنابراین لازم است همواره و بصورت مستمر مدیران سازمان نسبت به اثرات احتمالی یک ضعف امنیتی توجیه و دانش لازم در اختیار آنان قرار گیرد. در صورت بروز یک مشکل امنیتی در سازمان، مسئله بوجود آمده محدود به خود سازمان نشده و می‌تواند اثرات منفی متعددی در ارتباط با ادامه فعالیت سازمان را بدنبال داشته باشد.

۳-۲-۳- عدم تخصیص بودجه مناسب برای پرداختن به امنیت اطلاعات

مجاب نمودن یک مدیر سازمان مبنی بر اختصاص بودجه مناسب برای پرداختن به مقوله امنیت اطلاعات در سازمان از جمله مواردی است که چالش‌های خاص خود را خواهد داشت. مدیران، تمایل دارند بودجه را به حداقل مقدار خود برسانند، چراکه آنان یا اطلاعات محدودی در رابطه با تاثیر وجود ضعف‌های امنیتی در عملکرد سازمان را دارند و یا در برخی حالات بودجه، آنان را برای اتخاذ تصمیم مناسب محدود می‌نماید. با اختصاص یک بودجه مناسب برای پرداختن و بها دادن به مقوله امنیت اطلاعات در یک سازمان، پیشگیری‌های لازم انجام ودر صورت بروز مسائل بحرانی، امکان تشخیص سریع آنان و انجام واکنش‌های مناسب فراهم می‌گردد . بعبارت دیگر با در نظر گرفتن بودجه مناسب برای ایمن سازی سازمان، بستر مناسب برای حفاظت سیستم‌ها و داده‌های حساس در یک سازمان فراهم خواهد شد .

۳-۲-۴- اتکای کامل به ابزارها و محصولات تجاری

باید توجه داشته باشید که امنیت یک فرآیند است نه یک محصول که با خریداری آن خیال خود را در ارتباط با امنیت راحت نمائیم. مدیران سازمان لازم است شناخت مناسب و اولیه ای از پتانسل‌های عمومی یک فایروال و یا برنامه‌های ویروس یاب داشته باشند. ابزارهائی همچون فایروال و یا برنامه‌های ویروس یاب، بخشی از فرآیند مربوط به ایمن سازی اطلاعات حساس در یک سازمان بوده و با بکارگیری آنان نمی توان این ادعا را داشت که آنان سازمان را بطور کامل در مقابل تهاجمات، حفاظت خواهند نمود.

۳-۳- اشتباهات متداول کاربران معمولی

کاربران، به افرادی اطلاق می‌گردد که طی روز با داده‌ها ی حساس در یک سازمان سروکار داشته و تصمیمات و فعالیت‌های آنان، داده‌ها ی حساس و مقوله امنیت و حفاظت از اطلاعات را تحت تاثیر مستقیم قرار خواهد داد . در ادامه با برخی از اشتباهات متداولی که این نوع استفاده کنندگان از سیستم و شبکه مرتکب می‌شوند، اشاره می‌گردد.

۳-۳-۱- تخطی از سیاست امنیتی سازمان

سیاست امنیتی سازمان ، اعلامیه ای است که بصورت جامع، مسئولیت هر یک از کارکنان سازمان در ارتباط با امنیت اطلاعات و شبکه را تعریف و مشخص می‌نماید.هدف عمده اعلامیه فوق، ارائه روشی آسان بمنظور شناخت و درک ساده نحوه حفاظت سیستم‌های سازمان در زمان استفاده است.

کاربران معمولی، عموما تمایل به تخطی از سیاست‌های تدوین شده امنیتی در یک سازمان را داشته و این موضوع می‌تواند عاملی مهم برای تحت تاثیر قراردادن سیستم‌های حساس و اطلاعات مهم سازمان در مواجهه با یک تهدید باشد . [۶]

۳-۳-۲- ارسال داده حساس بر روی کامپیوترهای شخصی (منزل)

یکی از خطرناکترین روش‌ها در رابطه با داده‌های حساس موجود در یک سازمان، فعالیتی است که باعث غیر فعال شدن تمامی پیشگیری‌های امنیتی ایجادشده و درگیر شدن آنان در یک فرآیند غیر امنیتی می‌گردد . پرسنل سازمان عادت دارند، اطلاعات حساس سازمان را بر روی کامپیوتر منزل خود ارسال نمایند تا از این طریق امکان اتمام کار خود در منزل را پیدا نمایند. کاربران به این موضوع توجه نکرده اند که تغییر محیط ایمن سازمان با کامپیوتر منزل خود که دارای ایمنی به مراتب کمتری است، بطور جدی اطلاعات را در معرض آسیب و تهاجم قرار خواهد داد .[۹]

۳-۳-۳- دریافت فایل از سایت‌های غیر مطمئن

یکی از سرویس‌های اینترنت امکان دریافت فایل توسط کاربران است. دریافت فایل از وب سایت‌های گمنام و یا غیر مطمئن باعث کمک در توزیع برنامه‌های مهاجم در اینترنت می‌گردد. فایل‌ها و برنامه‌های دریافتی پس از آلودگی به نوع خاصی از برنامه مخرب (ویروس، کرم، اسب تراوا) می‌تواند تاثیرات منفی فراوانی را در ارتباط با عملکرد یک سازما ن بدنبال داشته باشد.[۱۰]

۳-۳-۴- عدم رعایت امنیت فیزیکی

میزان آگاهی و دانش کاربران در رابطه با رعایت مسائل ایمنی خصوصاً امنیت فیزیکی ، بطرز کاملاً محسوسی افزایش امنیت و حفاظت داده‌ها ی حساس در یک سازمان را بدنبال خواهد داشت. عموماً، رفتار کاربران در زمان استفاده از ایستگاه‌های کاری سازمان سهل انگارانه و فاقد سوادعمومی ایمنی است. به کاربران می‌بایست آموزش‌های لازم در رابطه با استراتژی‌های متفاوت بمنظور استفاده از سیستم‌های سازمان داده شود: مطمئن شوید آن‌ها قادرند بدرستی با اطلاعات حساس در سازمان برخورد نمایند و همواره پیامدهای عدم رعایت امنیت فیزیکی به آنان یادآوری گردد.[۱۰]

۴- نتیجه گیری

در این مقاله بعد از بررسی سیستم های اطلاعاتی، چالش‌ها و تهدیدهایی که می‌تواند توسط مدیران و کاربران این سیستم‌ها انجام شود و سیستم را دچار مشکل سازد بررسی شد. امید است با رعایت مسائل معرفی شده بتوان سیستم های اطلاعاتی امن و مطمئن تری داشته باشیم.

مرجع

[۱]عواجهی، مصطفی،"جنگ اطلاعات و عملیات روانی"، بانک مقالات و مطالب نظامی به زبان پارسی

[۲]فرشچی، علیرضا، عملیات روانی و جنگ نامتقارن، فصلنامه علمی- پژوهشی عملیات روانی، تابستان ۸۲، شماره ۲،ص ۲-۲۵

[۳]صادق زاده، سید حسن،"افزایش امنیت در بلوتوث با استفاده از روش های بیومتریک" کنفرانس ملی فناوری اطلاعات حال و آینده،دانشگاه آزاد واحد مشهد،۱۳۸۹

[4] Kate Farrise, Chinese Views of Information Warfare, Defense Intelligence Jouranal, Vol 10, Winter 2001 p. 38

[5] Joint Publication 1-02 ,Department of Defense Dictionary of Military and Associated Terms, 15 October ,۲۰۰۱ p. 209

[6] Libicki, Martin, What is Information Warfare?, National Defense University, ACIS Paper 3, August 1995, Preface, P.1

[7] Yoshihara ,Toshi, Chinese Information Warfare: A phan tom Menace or Emerging Threat ,November 2001. p.4

[8] Yoshihara, Toshi, Chinese Information Warfare: A phan tom Menace or Threat, November 2001. p. 1

[9]Libicki, Martin, What is Information Warfare?, NDU, ACIS paper3, August 1995, ch6

[10] Duan, Myriam, A, The Cyberspace Dimension in Armed Conflict, 2002, p.1