الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری

مجتبی درفشان[1]
علی جوانمرد[2]

تاریخ دریافت: ۱۳۹۵/۱۲/۱۴ تاریخ پذیرش: ۱۳۹۶/۰۱/۲۱

چکیده

تأمین امنیت اطلاعات سازمان‌ها در محیط امروزی که از شبکه‌های به‌هم‌پیوسته تشکیل‌شده کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ و جاسوسی این کار سخت‌تر نیز می‌شود. هدف اصلی این پژوهش، شناخت الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدهای سایبری است و محقق به دنبال پاسخ به این سؤال است که «الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری کدامند؟» و فرضیه اصلی شامل الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدهای سایبری، شامل الزامات سخت‌افزاری و نرم‌افزاری است، بوده است. این پژوهش از نظر نوع، کاربردی و از نظر روش به شیوه توصیفی– تحلیلی گردآوری شده است. روش گردآوری اطلاعات میدانی و کتابخانه‌ای بوده و ابزار گردآوری اطلاعات پرسش‌نامه محقق‌ساخته بوده است. جامعه آماری این پژوهش متشکل از مدیران، متخصصان و کارشناسانی است که با شبکه ملی ارتباطات، تهدیدات سایبری، اصول و مبانی پدافند غیرعامل آشنایی داشته و دارای مدرک کارشناسی ارشد به بالا و حداقل ۱۰ سال سابقه کار مرتبط باشند که تعداد آن‌ها ۱۰۰ نفر برآورد شده است. حجم جامعه نمونه به‌صورت تمام‌شمار همان ۱۰۰ نفر درنظر گرفته‌شده است. یافته‌های پژوهش حاکی از آن است که الزامات سخت‌افزاری شبکه ملی ارتباطات با رویکرد پدافند غیرعامل در مقابله با تهدیدات سایبری مرتبط با آن، استفاده از تجهیزات بومی همچون زیرساخت‌های بومی، ذخیره‌سازهای اطلاعات بومی، تجهیزات ارسال و دریافت بومی و الزامات سخت‌افزاری استفاده از نرم‌افزارهای بومی همچون نرم‌افزارهای ارسال و دریافت فایل و اطلاعات، ضدویروس‌ها و دیوار آتشین است.

واژگان کلیدی: *پدافند غیرعامل، اصول پدافند غیرعامل، امنیت سایبری، فناوری اطلاعات*

---

۱. عضو هیئت علمی دانشکدهٔ علوم و فنون فارابی (E- mojtabaderafshan@gmail.com)
۲. پژوهشگر علوم سیاسی و دانش‌آموخته کارشناسی ارشد دانشکدهٔ علوم و فنون فارابی، نویسنده مسئول (E-jawvnmarda@gmail.com)

مقدمه

فضای سایبر مجموعه‌ای متشکل از زیرساخت‌ها، شبکه‌ها، نرم‌افزارها، سخت‌افزارها، پروتکل‌ها، محتوا و سیاست‌های حاکم بر این حوزه است. همچنین این فضا، مجموعه‌ای از مفاهیم را در قالب محتوای فرهنگی، سیاسی یا حتی منابع مادی و مالی و منابع حقوقی و معنوی را دربرمی‌گیرد. استفاده از فناوری‌های فضای سایبر با توجه به رویکردهای جدید در دنیای کنونی امری اجتناب‌ناپذیر است. با نگرش به اینکه قواعد و ابزار فضای سایبر در اختیار دیگران است، بازیگر یا کشوری که می‌خواهد وارد این عرصه شود باید تلاش کند که از همه ظرفیت‌ها، نقاط مثبت و فرصت‌های آن استفاده کند و با تهدیدات موجود در این فضا مبارزه نموده و بیشترین بهره‌برداری لازم را از این فضا داشته باشد. این مهم بدون داشتن ساختار مناسب جهت مقابله با تهدیدات این حوزه امکان‌پذیر نیست.

بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهم‌ترین آن‌ها عبارت‌اند از: جنگ سایبری، تروریسم سایبری، جرائم سایبری و آشفتگی سایبری و ... .

در کشور ما بسیاری از نرم‌افزارهای پایه از قبیل سیستم‌عامل و نرم‌افزارهای کاربردی و اینترنتی از طریق واسطه‌ها و شرکت‌های خارجی تهیه و تأمین می‌شود، ازاین‌رو احتمال نفوذ از طریق حفره‌های مخفی موجود در این برنامه‌ها وجود دارد. غفلت از این حفره‌ها موجب بروز خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. با توجه به مطالب اشاره شده، چنانچه یک پیام خاص به‌عنوان مثال از سوی یک شرکت تولیدکننده نرم‌افزار در جهان، به کلیه سامانه‌های متصل به شبکه که از این نرم‌افزار استفاده می‌کنند فرستاده شود و نرم‌افزار مذکور در پاسخ به این پیغام، موجب خرابی سیستم شده و یا بخشی از اطلاعات را از بین ببرد، چه ضررهای هنگفتی به امنیت و اقتصاد کشور وارد خواهد شد؟ به‌عنوان‌نمونه شرکت «چک پوینت» که یکی از برترین شرکت‌ها در زمینه تولید نرم‌افزارهای امنیتی در جهان است، شعبه اصلی آن در رژیم اشغالگر قدس قرار دارد.

همان‌گونه که مطرح شد امنیت شبکه در هر کشوری از اهمیت ویژه‌ای برخوردار بوده و کشور ما نیز باید به آخرین فناوری‌های امنیت شبکه مجهز شود و ازآنجاکه این فناوری‌ها به‌صورت محصولات نرم‌افزاری قابل خریداری نیستند، بایستی محققین کشور این مهم را در دست بگیرند. گسترش روزافزون اینترنت و نفوذ این فناوری به

زندگی روزمره افراد در سراسر جهان موجب شده هر کس بدون توجه به محل زندگی، ملیت، شغل، زبان و بدون محدودیت زمانی به اطلاعات در سطح اینترنت دسترسی داشته باشد و از آن استفاده کند. باتوجه‌به تغییر راهبردهای جنگی استکبار جهانی (از جنگ سخت به نرم) و انهدام زیرساخت‌ها برای درهم شکستن پایداری کشورها، میدان جنگ به تمام ارکان حیاتی کشورها به‌ویژه حوزه‌های اقتصادی کشانده شده است. یکی از این راهبردها، تزریق کدهای مخرب و جاسوس‌افزارها درون شبکه رایانه‌ای سازمان‌ها و دستگاه‌های مهم و زیرساختی کشور، با هدف ایجاد وحشت، خسارت اقتصادی و ازبین‌بردن ثبات و پایداری کشورهاست که با هزینه‌ای اندک انجام می‌شود و در طول تاریخ به‌وسیلهٔ دولت‌ها یا سازمان‌های تروریستی مستقل و تابع دولت‌های خاص، انجام شده است.

بیان مسئله

شبکه‌های رایانه‌ای یکی از فناوری‌های جذابی هستند که توانسته‌اند توجه بسیاری را به‌سوی خود جلب نمایند و عده‌ای را نیز مسحور خود نموده‌اند. این فناوری جذابیت و موارد کاربرد بالایی دارد ولی مهم‌ترین مرحله که تعیین میزان رضایت از آن را به دنبال خواهد داشت ارزیابی نیازها و توقعات و مقایسه آن با امکانات و قابلیت‌های این فناوری است. مهم‌ترین مسئله‌ای که در هر شبکه رایانه‌ای قابل‌توجه است، ضریب اطمینان و امنیت آن در مقابل عوامل داخلی و خارجی است. هم راستا با حرکت به سمت یک سازمان مدرن و مبتنی بر فناوری اطلاعات، می‌بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری است. وپایش دستیابی و نحوهٔ استفاده از منابع به اشتراک گذاشته‌شده، از مهم‌ترین اهداف یک سیستم امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای به ویژه اینترنت، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته‌شده، وارد مرحله جدیدی شده است. دراین‌راستا، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک خط‌مشی خاص پایبند بوده و بر اساس آن سیستم امنیتی را اجرا و پیاده‌سازی نماید. ایجاد ننمودن سیستم مناسب امنیتی، می‌تواند پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. راهبردسازمان‌ها و نهادهای

دولتی و خصوصی برای حفاظت و دفاع از اطلاعات چیست؟ درحالی‌که یک سازمان برای خرید سخت‌افزار نگرانی‌های خاص خود را داشته و سعی در برطرف نمودن معقول آن‌ها دارد، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی به‌مراتب بیشتری در سازمان وجود داشته باشد؟

اغلب مردم وقتی به گزینه نظامی علیه ایران فکر می‌کنند حمله آمریکا و دیگر کشورهای متخاصم به تأسیسات اتمی مهم ایران واقع در نطنز، فردو، اراک و اصفهان را در نظر می‌آورند. آن‌ها انتظار دارند ایران در پاسخ به این اقدام تنگه هرمز را ببندد، موشک‌هایش را به سمت رژیم صهیونیستی پرتاب کند و یا حملات تروریستی علیه نیروهای آمریکایی مستقر در عراق یا افغانستان انجام دهد؛ ولی اگر این حملات به شکل حمله سایبری بدون نامی باشد که بورس سهام منطقه‌ای ایران را برای چند ساعت مختل کند، شرایط به چه ترتیب خواهد شد؟ اگر حمله موجب قطع جریان برق در شهرهای بزرگ کشور، مختل شدن خطوط حمل‌ونقل هوایی یا تداخل با حملات نظامی بیشتر علیه ایران از طریق مخابره اطلاعات غلط به فرماندهان نظامی آمریکا بشود چه رخ خواهد داد؟

در این پژوهش به دنبال بررسی این مسئله هستیم که آیا شبکه ملی اطلاعات با به‌کارگیری الزامات تعیین‌شده از آموزه‌های پدافند غیرعامل می‌تواند از بروز حملات سایبری از سوی کشورهای دیگر علیه نظام جمهوری اسلامی ایران جلوگیری به عمل آورد؟ میزان آسیب‌پذیری این شبکه تا چه حد است؟ آیا شبکه ملی اطلاعات قابل‌اجرا و پیاده‌سازی به‌صورت عملی است؟ اجرای شبکه ملی اطلاعات از لحاظ اقتصادی توجیه دارد یا خیر؟ و اینکه به‌منظور جلوگیری از آسیب‌های حملات سایبری از سوی تبهکاران می‌توان به شبکه ملی اطلاعات اطمینان کرد یا باید به دنبال راهکار دیگری بود؟ دغدغه اصلی محقق این است که کار علمی مدون با رویکرد پدافند غیرعامل در این خصوص وجود ندارد.

ضرورت و اهمیت پژوهش

۱- حضرت آیت‌الله‌العظمی امام خامنه‌ای (مدظله‌العالی) در رابطه با تهدید نرم دشمن می‌فرمایند: امروز آرایش تهاجمی فرهنگی بسیار خطرناکی علیه انقلاب به‌وضوح مشاهده می‌شود، زیرا جهان اسلام بیدار و هوشیار شده است. ازاین‌رو تهاجم فرهنگی دشمن با گذشته تفاوت بسیار دارد و شکل جدیدی پیدا کرده است و برای مقابله با آن باید با شناخت و آگاهی کامل عمل کنیم (۲۰ آذر ۱۳۷۰ در جمع شورای عالی فرهنگی کشور).

۲- فناوری اطلاعات فرصت‌های بی‌نظیری در اختیار بشریت قرار داده است ولی مشابه هر فناوری نوظهور در جهان، چالش‌هایی را نیز به دنبال دارد. سرقت اطلاعات، خرابکاری،

ازکاراندازی سامانه‌های رایانه‌ای، کلاهبرداری و جاسوسی ازجمله تأثیرات مخرب فناوری اطلاعات برای حیات بشری است.

۳- توسعه اینترنت در جوامع و گسترش آن حتی به درون منازل و محل‌های کار مردم و نیز جهان‌شمول بودن و وجود خطرات بالقوه آن، سازمان‌ها و دولت‌ها را با چالش‌های جدیدی روبه‌رو ساخته است.

۴- فناوری ارتباطی و اطلاعاتی به زیرساخت‌های مهم قدرت پنهان و ملایم دیپلماسی عصر نوین تبدیل‌شده است. در چنین فضایی، اطلاعات، از مهم‌ترین عوامل قدرت‌ساز در جوامع است. قدرت اطلاعات از فناوری اطلاعات و ارتباطات و مضمون اطلاعات تشکیل می‌شود. فناوری اطلاعات و ارتباطات مردم را قادر می‌سازد با یکدیگر تعامل داشته، اطلاعات را گسترده‌تر، سریع‌تر، ارزان‌تر و راحت‌تر جمع‌آوری و منتشر کنند. پس فناوری اطلاعات و ارتباطات، نیروی محرک انقلاب اطلاعاتی است.

اهمیت

۱- پیش‌بینی اقدامات مقابله‌ای با خرابکاری یا جاسوسی و یا دست‌کاری داده‌ها -استفاده غیرمجاز از اینترنت- نشت ناخودآگاه اطلاعات و ... با دیوارهای آتش، سامانه تشخیص نفوذ، سامانه یا لایه که به‌طور نظام‌مند به مقابله با مسائل بالا برمی‌خیزد.

۲- مقابله با تهدیدهای اینترنتی جدید با وضع آئین دادرسی حقوقی جدید ویژهٔ فضای مجازی.

۳- مقابله با چالش‌های امنیتی کلان که به‌واسطهٔ ویژگی‌های یادشده بالا خطرات زیادی را برای کشور خواهد داشت.

۴- پیداکردن آمادگی برای مقابله با تهدیدهای خارجی از ناحیه کسانی که به بخش‌های نظامی و آژانس‌های امنیتی کشورهای خارجی و حتی شرکت‌هایی که وابستگی زیادی به آن کشورها دارند، در تعامل هستند.

۵- توجه بیشتر به آسیب‌پذیری خطوط اطلاعاتی دیجیتالی کشور که امنیت و استاندارد شبکه در سطوح عالی رعایت نمی‌شود و توجه بیشتر به اقدامات خرابکارانه دشمن.

۶- توجه بیشتر به سیاست‌گذاری‌های فضای مجازی و بازبینی سیاست‌های جاری.

پیشینه پژوهش

۱- وزارت پست و تلگراف و تلفن در سال ۱۳۸۱، در تهران گزارش کاربردی با عنوان سند راهبردی توسعه فناوری و اطلاعات منتشر کرده است که نتیجه آن بررسی وضع موجود اطلاعات و ارتباطات ملی، بررسی نقاط ضعف، قوت، تهدید و فرصت، چشم‌انداز و راهبردهای توسعه فناوری اطلاعات و ارتباطات ملی و برنامه‌های اجرایی فناوری اطلاعات و ارتباطات ملی را به همراه داشته است.

۲- سعید کافی در سال ۱۳۹۳، در دانشگاه عالی دفاع ملی تهران، رساله دکتری با عنوان الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری را انجام داده است که نتایج آن حاکی از آن است که الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری تدوین راهبرد در پنج مؤلفه انسانی، فرایندها، احراز هویت، یکپارچه‌سازی فرماندهی و کنترل شبکه‌ها است.

۳- حسین انتظامی در سال ۱۳۹۰، در دانشگاه عالی دفاع ملی تهران رساله دکتری تحت عنوان تأثیر فناوری اطلاعات و ارتباطات بر امنیت ملی انجام داده است که نتایج آن حاکی از آن است که ۱- فناوری اطلاعات و ارتباطات علاوه‌بر مؤلفه‌ها بر زمینه‌ها و لایه‌های امنیت ملی هم تأثیر دارد. ۲- فناوری اطلاعات و ارتباطات صرفاً سخت‌افزاری و زیرساخت ارتباطی و اطلاعاتی نیست.

۴- مصطفی اصلانی مقدم در سال ۱۳۸۵، در دانشگاه عالی دفاع ملی تهران رساله دکتری خویش را با عنوان جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی ج.ا.ا به سرانجام رسانیده است که نتایج آن حاکی از آن است که به‌منظور افزایش قدرت نظامی لازم است اقدامات اساسی درخصوص تدوین راهبردهای منطقی و کاربردی، تدابیر مناسب و راهکارهای مطلوب مرتبط با هر زمان در بخش‌های نظامی و سایبری مدنظر قرار گیرد.

۵- سیروس الوندی در سال ۱۳۹۲، در دانشکدهٔ علوم و فنون فارابی تهران پایان‌نامه کارشناسی ارشد خود را تحت عنوان الزامات پدافند غیرعامل در حملات سایبری انجام داده است که نتایج آن حاکی از آن است که سازمان پدافند غیرعامل نسبت به تدوین برنامه‌های منطقی و کاربردی برای ساختارها و تجهیزات اقدام کند. وزارت دفاع و پشتیبانی نیروهای مسلح به‌عنوان متولی کارها، محورها، ضوابط و زیرساخت‌ها را مشخص کند.

۶- مقاله‌ای با عنوان «تهدیدات سایبری و تأثیر آن بر امنیت ملی» توسط علی خلیل‌پور رکن‌آبادی و یاسر نورعلی‌وند در سال ۱۳۹۱ در دانشگاه مالک اشتر تهران ارائه شده است که نتیجه آن داشتن ویژگی‌هایی مانند قیمت پایین، گمنامی و تأثیرگذاری شگرف انتشار قدرت را

به همراه خواهد داشت که نه‌تنها باعث شده که دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت برخوردار شوند بلکه منجر به ورود بازیگران دیگری همچون شرکت‌ها و گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی گردند. بنابراین این پدیده امنیت ملی را از ابعاد، مفهوم، دولت‌محوری، بعد جغرافیایی و گستردگی شیوه مقابله با تهدیدات و فراوانی بازیگران تحت تأثیر قرار داده است.

هدف اصلی: شناخت الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری.

سؤال اصلی: الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری کدامند؟

فرضیه اصلی: الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری، شامل الزامات سخت‌افزاری شامل استفاده از تجهیزات بومی همچون زیرساخت‌های بومی، ذخیره‌سازهای اطلاعات بومی، تجهیزات ارسال و دریافت بومی و نرم‌افزاری شامل استفاده از نرم‌افزارهای بومی همچون نرم‌افزارهای ارسال و دریافت فایل و اطلاعات، ضدویروس، دیوار آتشین بوده است.

پیشینه

مفهوم‌شناسی فضای سایبری

فضای سایبر[1]: عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. واژه سایبر از لغت یونانی کی‌برنتس[2] به معنی سکان‌دار یا راهنما مشتق شده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی گفته می‌شود. فضای مجازی جهانی موازی با جهان واقعی است که همه وجوه تکرارشوندهٔ زندگی در جهان واقعی را شامل می‌شود و به گفتهٔ دکتر عاملی فرایندی است که به همگن‌سازی با جهان واقعی می‌انجامد. (واحدی، ۱۳۹۳: ۲۳۶)

فضای سایبر در ایران: با توجه به اینکه در ایران، ضدتبلیغ‌های فراوان در رابطه با اینترنت و فضای مجازی وجود دارد، به‌نظر می‌رسد مهم‌ترین برنامهٔ ایران در رابطه با استفاده از کاربردهای این شبکه جهانی، حذف این ضدتبلیغ‌ها، گسترش و فراگیرکردن آن در راستای استفاده از آن است؛ زیرا تنها در این صورت است که استفاده از سودمندی‌های آن در همهٔ

1. Cyberspace
2. Kybernetes

زمینه‌ها و شاخه‌ها از برنامه‌ریزی‌های کوچک تا بزرگ مثل کاهش ترافیک تا آموزش‌های مختلف (شخصی و همگانی) امکان‌پذیر خواهد بود. (زرقانی، ۱۳۹۲: ۱۳۲).

ویژگی‌های فضای سایبر: در اواسط دهۀ ۹۰ گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرائم رایانه‌ای، با عنوان جرائم سایبری (مجازی) یا جرائم در محیط سایبر شکل گرفته است. به‌این‌ترتیب جرائم اینترنتی را می‌توان مکمل جرائم رایانه‌ای دانست، به‌خصوص‌اینکه جرائم نسل سوم رایانه‌ای که به جرائم در محیط مجازی معروف است، غالباً از طریق این شبکه جهانی به وقوع می‌پیوندد. کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون درنظرگرفتن اینکه، اطلاعات و خدمات در کدام نقطه دنیا واقع شده است. محیط سایبر زمینه فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیۀ معاملات تجاری در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده است. محدودۀ فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و در یک سطح کم‌هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد. (واحدی، ۱۳۹۳: ۶۴)

جرائم در فضای سایبر: فضای سایبر هنوز در مراحل اولیه است. طبیعت این جرائم و سوءاستفاده‌های مرتکب‌شده در این دنیای مجازی جدید، امنیت ناکافی، انتشار سریع اطلاعات، فرصت‌های بالقوه مورد سوءاستفاده افراد شرور است. در فضای سایبر برای جست‌وجو و پیداکردن جرائم مشکلات پیچیده‌تر می‌شود. در دنیای واقعی دزدی از بانک کاملاً مشخص است چراکه بعد از سرقت در خزانه بانک پولی موجود نیست ولی در فناوری رایانه‌ای شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود. برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان‌طور که دقیقاً بوده باقی بگذارد. در فضای سایبر کپی عیناً عین اصل است. با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی را مثل پاک کردن اثرانگشت را تغییر دهد. (دوست محمدیان، ۱۳۹۲: ۶۷).

مجرمین فضای سایبر

رخنه‌گرها[1]: در دهه ۱۹۷۰ واژه رخنه‌گر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر و باهوش باشد. این درست است که رخنه‌گرهای کنجکاو می‌توانند سهواً باعث زیان‌های قابل‌توجهی شوند، اما جست‌وجو برای یافتن اطلاعات و آموزش، نه انتقام‌گیری یا صدمه زدن

1. Hackers

به دیگران، عاملی است که باعث می‌شود اکثر رخنه‌گرها سردرگمی خود را به نحوی بی‌رحمانه دنبال کنند.

قفل‌شکن‌ها[1]: از سوی دیگر قفل‌شکن‌ها رخنه‌گرهای بدخواهی هستند. آن‌ها به سامانه‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر کنند، فایل‌ها را پاک کنند یا بعضی انواع دیگر ویرانی را به‌بار آورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی قفل‌شکن‌ها است.

فریک‌های تلفن: شکل دیگر از جرائم رایانه‌ای را «فریک‌های تلفن» مرتکب می‌شوند. فریک‌ها به‌جای دسترسی به سیستم‌های رایانه‌ای، از طریق خطوط تلفن در دنیای سایبر گشت می‌زنند.

بحران‌سازهای فضای سایبر

ویروس: ویروس یا برنامه‌های خود همانندساز، برنامه‌هایی هستند که با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند و معمولاً از طریق یک دیسکت و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند.

عنکبوت‌های موتورهای جست‌وجو و پالس‌های الکترومغناطیس: که می‌توانند دیسک سخت یک رایانه را ذوب کنند.

کرم‌ها: می‌توانند به یک سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه، برای مثال از طریق یک دیسکت، گسترش پیدا کنند. کرم‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه رایانه کند شود یا از کار بیفتد.

بمب‌های منطقی: آن‌ها تعمداً زیان‌بار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند. آن‌ها طوری طراحی‌شده‌اند که طی یک دوره زمانی در رایانه غیرفعال باقی می‌مانند و با سر رسیدن تاریخی که برنامه آن‌ها مشخص‌شده است منفجر می‌شوند (دوست محمدیان، ۱۳۹۲: ۱۳).

انواع جرائم سایبری: تنوع انواع جرائم ارتکابی در فضای سایبر شامل جرائم نسل اول رایانه‌ای (البته به شکل نوین) و یک سری جرائم بسیار جدید و بی‌سابقه است.

جاسوسی رایانه‌ای: جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشا و انتقال و استفاده از اسرار است. فرد مرتکب جرم با دستیابی و فاش کردن این اسرار، ضرر سیاسی، نظامی، مالی و تجاری می‌کند. این جرم امنیت ملی را با مخاطره مواجه می‌کند.

1. Crackers

خرابکاری رایانه‌ای[1]: این جرم با جرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی و اقتصادی یک کشور و بالطبع اخلال در امر حکومت است.

جعل رایانه‌ای: واردکردن، تغییر، محو یا متوقف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای برای اهداف سیاسی و اقتصادی صورت می‌گیرد. جعل رایانه‌ای جعل داده‌هاست. در جعل رایانه‌ای عمل ارتکابی بر داده‌ها اثر می‌گذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.

افترا و نشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین و گسترده‌ترین سرویس شبکه‌های رایانه‌ای و بین‌المللی است، هر کاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک نشانی مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به‌آسانی در آن تقلب کرد. این قابلیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعات برای تهیه‌کننده کاملاً مشکل است و در عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی و گسترده امنیتی مشکل بوده و تنها برای بخش کوچکی از داده‌ها میسر است.

پولشویی نامشروع پول: به‌دست‌آوردن پول از طریق غیرقانونی یا پول کثیف، به‌نحوی‌که قانونی یا پاک به نظر برسد، از جرائم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد.

جرائم ناظر به کپی‌رایت و برنامه‌ها: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش و استفاده غیرمجاز از برنامه‌های رایانه‌ای را سرقت نرم‌افزار گویند.

تأمین خط‌مشی اصول حفاظت در فناوری اطلاعات و ارتباطات

آسیب‌پذیری زیاد و زیان‌های سنگین مشکلات فناوری اطلاعات باعث زیادشدن فشار بر روی مدیران فناوری اطلاعات برای انجام کارهایی برای جلوگیری از ضرر و زیان سازمانی و به حداقل رساندن خطرات احتمالی است که این نیز یکی از اصول پدافند غیرعامل آن سازمان خواهد بود. از مشکلات امنیتی داده‌ها در فناوری اطلاعات می‌توان به آلوده‌شدن به انواع ویروس‌ها، نفوذگران اینترنتی، جاسوسان داخلی که از طریق شبکه‌های محلی صورت می‌گیرد و یا مشکلاتی که در اثر خرابی سخت‌افزارها به‌وجود می‌آید و باعث ازبین‌رفتن داده‌های آن سازمان می‌شود. راهکارها و رهنمودهایی که برای حل این مشکلات ارائه می‌شود عبارت‌اند از: مجهز

1. Computer Sabotage

کردن سامانه‌های فناوری اطلاعات به ویروس‌شناس‌ها و سیستم‌عامل‌ها و برنامه‌های ضدجاسوسی و تهیه دیسک‌ها و نوارهای پشتیبان از کلیه داده‌های مهم در فواصل زمانی منظم و نگهداری آن‌ها در اماکن خواهد بود.

خطرهای تهدیدکنندهٔ سیستم فناوری اطلاعات در فضای سایبر: خطرهای تهدیدکنندهٔ سامانه‌های فناوری اطلاعات در فضای سایبر به دو دستهٔ عمدی و غیرعمدی تقسیم می‌شوند، خطرهای عمدی خطرهایی هستند که امنیت اطلاعات سیستم را با برنامه‌های قبلی و هدفی خاص موردحمله قرار می‌دهند: مثل خطر رخنه‌گرها؛ و خطرهای غیرعمدی خطرهایی هستند که بر اثر اشتباهای انسان و نیروی کار به سیستم وارد می‌شوند که این نوع خطر بیش‌ترین میزان خسارت را به سیستم اطلاعاتی وارد می‌کنند. برای اینکه در سیستم‌ها بتوانیم خطرهای موجود را رفع کنیم، قبل از هر چیز باید به فکر ایجاد امنیت شبکه‌های اطلاعاتی خود باشیم این ایجاد امنیت ابتدا باید شامل اتخاذ سیاست‌های امنیتی باشد. مواردی که یک سازمان برای پیاده‌سازی یک سیستم مدیریت امنیتی اعمال می‌کند به شرح زیر است:

تعیین سیاست امنیتی، اعمال سیاست‌های مناسب، بررسی بلادرنگ وضعیت امنیت اطلاعاتی بعد از اعمال سیاست امنیتی، بازرسی و آزمون امنیت شبکهٔ اطلاعاتی، بهبود روش‌های امنیت اطلاعاتی سازمان که این تهدیدات به‌وسیلهٔ یک سیستم مدیریت امنیت اطلاعات قابل‌پیشگیری است.

مجموعه واپایش امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی: تدوین سیاست امنیتی سازمان، ایجاد تشکیلات تأمین امنیت سازمان، دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم، امنیت کارکنان، امنیت فیزیکی و پیرامونی، مدیریت ارتباطات.

کنترل دسترسی: در این قسمت، نیازمندی‌های کنترل دسترسی، نحوه مدیریت دسترسی کارکنان، مسئولیت کاربران، ابزارها و سازوکارهای کنترل دسترسی در شبکه، کنترل دسترسی در سیستم‌عامل‌ها و نرم‌افزارهای کاربردی، استفاده از سیستم‌های پایش‌گری و کنترل در ارتباط از راه دور به شبکه ارائه‌شده است، نگهداری و توسعه سیستم‌ها، مدیریت تداوم فعالیت سازمان، پاسخگویی به نیازهای امنیتی است.

بررسی انواع حملات سایبری در حوزه فناوری اطلاعات و ارتباطات

الف- حملات خاموش: این حملات شامل فعالیت‌هایی می‌شوند که در آن‌ها بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم‌های آسیب‌پذیر به آن‌ها نفوذشده و منجر به سوءاستفاده از منابع سیستم می‌گردد.

ب- حملات فعال: این حملات، حملاتی هستند که به سامانهٔ رایانه‌های زیرساخت‌های حیاتی نفوذ می‌کنند و می‌توانند اطلاعات حساس را دست‌کاری کنند و باعث بروز حوادث و فجایع ملی و جبران‌ناپذیر گردند. از اهداف آن‌ها می‌توان ازکارانداختن شبکه‌های خدماتی عمومی مثل شبکه برق، گاز، داده و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد.

کالبدشناسی و مراحل یک حمله

۱. ابتدا یک هدف مشخص تعیین می‌شود که می‌تواند قسمتی از یک ساخت حیاتی مانند شبکه راه‌آهن، شبکه برق، شبکه ای‌تی‌ام و یا وبگاه‌های دولتی باشد.

۲. مهاجم‌ها شروع به جمع‌آوری اطلاعات از طریق شبکه اینترنت، مقالات، مطالعات، وبگاه‌های هدف، انجام آزمایش‌های آزمون نفوذ بر روی وب، شناسایی مؤلفه‌های فن هدف مانند سیستم‌عامل، شناسایی زیرساخت شبکه، جمع‌آوری اطلاعات از طریق مهندسی اجتماعی (توسط کارکنانی که در آن ساختار شاغلند)، می‌کنند.

۳. حمله سایبر اتفاق می‌افتد.

۴. پژوهش و بررسی برای حملات دیگر انجام می‌گیرد.

نگاهی به چهارچوب و مبانی پدافند غیرعامل کشور

تعاملات انسانی و روابط میان کنش‌گران عضو نظام بین‌الملل همواره در یک بستر و بافت حادث می‌شود. ویژگی‌ها و مؤلفه‌های بنیادین هر بافتی، نقش مهمی را در شکل‌دهی و جهت‌دهی به رفتارها و نحوهٔ تعامل میان واحدهای در حال تعامل اعم از فرد یا دولت بازی می‌کند. در همین چهارچوب، والتر، نظام بین‌المللی آنارشیسم را با رفتار مفروضی در نظر می‌گیرد که دولت‌ها در بستر آن به تعامل با یکدیگر می‌پردازند و رفتار دولت‌ها، ازجمله تلاش برای افزایش قدرت از طریق خودیاری و یا اتحاد با دولت‌های همسو، درنتیجه آنارشیک بودن نظام بین‌المللی است. (ناصری، ۱۳۸۸: ۴۵). برخی ازنظریه‌پردازان روابط بین‌الملل و علوم ارتباطات، روندها و تحولات جامعه انسانی، ازجمله امور نظامی و ارتباطات میان افراد را به‌گونه‌ای نظریه‌پردازی کرده‌اند که نقش مستقلی برای فناوری قائل شده‌اند و در همین راستا کوشیده‌اند نقش فناوری را در تحولات حوزه‌های خاص از قلمرو فعالیت بشری مطالعه نمایند.

مارشال مک لوهان[1] استدلال می‌کند رسانه‌های هر عصر ماهیت جامعه آن عصر را تعیین می‌کنند. از دید مک لوهان، پیشرفت هر جامعه‌ای هم‌زمان با رشد فناوری‌ها بوده است. جوامع

1. Marshall Mc Luhan

انسانی از رسانه‌ها (فناوری) از حروف الفبا تا اینترنت، تأثیر پذیرفته و بر آن‌ها تأثیر نهاده‌اند. ازآنجاکه ما به تهدیدات سایبر تروریستی علیه امنیت ملی توجه داریم، باید مباحث خود را بر فناوری‌های مرتبط با ظهور تهدیدات نوین، یعنی روش‌ها، ابزارها و مهارت‌هایی متمرکز سازیم که فرصت‌ها و محدودیت‌هایی را برای کنش‌گرانی از قبیل دولت‌ها و بازیگران غیردولتی ایجاد می‌کنند؛ روش‌ها و ابزارهایی که کنش‌گران برای اعمال تهدید علیه یکدیگر و الگوهای منازعه در سطوح مختلف به‌کار می‌برند. علاوه‌براین، ظهور فناوری‌های نوین که از سطح واحدها شروع می‌شود و به‌تدریج جهان‌گستر می‌شود بر ابعاد سیاسی، اجتماعی و اقتصادی نظام سیاسی داخلی و بین‌المللی تأثیر می‌نهد. از دیدگاه واقع‌گرایی ساختاری، اهداف دولت‌ها و نیاز آن‌ها به توانمندی‌های نظامی، سیاسی و اقتصادی برای تحقق این اهداف کم‌وبیش تغییرناپذیرند. مادامی‌که آنارشی بین‌المللی وجود دارد، دولت‌ها به دنبال این توانمندی‌ها هستند؛ اما توانمندی‌های اقتصادی، سیاسی و نظامی خاصی که دولت‌ها برای تحقق اهداف ازجمله امنیت در دوره‌های خاص به آن‌ها نیاز دارند، به‌مرورزمان تغییر می‌کند. نوآوری‌های فناورانه بر آنارشی بین‌المللی یا موجودیت و کارویژه‌های بنیادین دولت‌ها غلبه نکرده‌اند، اما برخی از نوآوری‌های فناورانه تأثیرات ژرفی بر برآیندهای سیاسی داخلی و بین‌المللی داشته‌اند.

روند شتابان گسترش و پراکندگی فناوری‌های اطلاعات و ارتباطات، جهان را در بستر بافت پسابین‌المللی یا پساوستفالیایی قرار داده است. این وضعیت بر تمامی ابعاد حیات بین‌المللی سایه افکنده و تمامی سطوح فردی، فروملی، ملی، منطقه‌ای و بین‌المللی را درنوردیده است (Iopresti, 2005: 113).

برهمین‌اساس، گسترش فناوری‌های اطلاعات و ارتباطات و کاربست آن در تمامی قلمرو حیات بشری، جایگاه فناوری را در حوزه‌های سیاسی، اقتصادی و اجتماعی برجسته ساخته است، به‌گونه‌ای‌که بافت فناورانه‌ای را پدید آورده است که روندها و پویش‌های عرصه داخلی و بین‌المللی از آن تأثیر چشمگیری می‌پذیرند. ازآنجاکه هستی‌شناسی نظریه‌های متعارف روابط بین‌الملل بر مبنای جهان واقعی شکل می‌گیرد، درنتیجه بافت فناورانه به‌عنوان بستر پویش امنیت مورد بی‌توجهی قرار می‌گیرد. محیط بین‌الملل به‌جای بافت فناورانه می‌نشیند و دو کارویژه‌ای می‌شود: نخست این‌که عرصه بین‌المللی بستر امنیت است و دوم در برابر عرصه داخلی قرار داده می‌شود. پایه استدلال پژوهش حاضر این است که نه نوع تعامل عرصه داخلی و بین‌المللی، بلکه این بافت فناورانه است که پویش‌های امنیتی را شکل می‌دهد و این‌که چه فناوری در سطح وسیع‌تری گسترش یابد، بیشتر امنیت را دستخوش دگرگونی می‌سازد. این مدعا به‌ویژه دربارهٔ گسترش فناوری‌های اطلاعات و ارتباطات صادق است؛ چراکه فناوری‌های

اطلاعات و ارتباطات با گسترش خود، جهان واقعی را درنوردیده‌اند و فضای مجازی را پدید آورده‌اند؛ البته به بیان صحیح‌تر، فضای مجازی را برجسته ساخته‌اند و بر تأثیرگذاری آن افزوده‌اند. ویژگی بارز فضای مجازی برخلاف جهان واقعی، نامتناهی بودن، گمنام‌سازی، سیال بودن و کنترل‌ناپذیری یا به بیان دقیق‌تر سخت کنترل‌پذیری آن است. گسترش فناوری‌های اطلاعات و ارتباطات و تمایل فزایندهٔ دولت‌ها برای بهره‌گیری از این فناوری‌ها به‌منظور انجام کارویژه‌های امنیتی، سیاسی و اقتصادی، جایگاه فضای مجازی را در دنیای امروزی بسیار برجسته ساخته است، به‌گونه‌ای‌که فضای مجازی اهمیتی هم‌پای جهان واقعی یافته است؛ بنابراین امنیت را دیگر نمی‌توان با ویژگی‌های سنتی که بیشتر مبتنی بر ویژگی‌های جهان فیزیکی است، تعریف کرد. چراکه فناوری‌های اطلاعات و ارتباطات، قوام‌بخش بافت فناورانه‌ای هستند که پویش‌های امنیتی در آن متفاوت با ویژگی‌های جهان فیزیکی است. در این بافت فناورانه، مرزهای مستحکم عرصه داخلی و عرصه بین‌المللی بسیار کمرنگ می‌شود، به‌طوری‌که کنترل دولت‌ها بر جریان اطلاعات، در طول مرزهای سرزمینی از بین می‌رود، چراکه بخش قابل‌توجهی از فعالیت‌های نظامی، اقتصادی و فرهنگی کنش‌گران غیردولتی در فضای مجازی و با بهره‌گیری از امکانات فناوری‌های اطلاعات و ارتباطات انجام می‌گیرد. در این چهارچوب یکی از مهم‌ترین تهدیداتی که در بافت فضای مجازی ظهور کرده، سایبر تروریسم است که نه‌تنها به‌وسیله بازیگران غیردولتی مورداستفاده قرار می‌گیرد، بلکه دولت‌ها نیز از آن به‌عنوان ابزاری برای دستیابی به اهداف خود استفاده می‌کنند.

بازدارندگی و دفاع غیرعامل: دولت‌ها زمانی به اعمال بازدارندگی روی می‌آورند که بخواهند دیگر کشورها را از انجام اقدامات مضر به منافع خود منصرف نمایند، اعمال بازدارندگی اغلب با مشکلاتی مواجه است. بااین‌وجود، در مقایسه با اعمال زور که به‌معنای وادار ساختن کشورها به اتخاذ رویارویی معین و یا پرهیز از چنین رویارویی است، آسان‌تر است. روش‌های دستیابی به بازدارندگی به شرح زیر است: اعمال مجازات سخت[1]، تحذیر[2]، تجدید اطمینان[3] و سازش[4] بوده است. (حسن بیگی، ۱۳۸۴: ۱۳۲).

پدافند غیرعامل در حوزه فناوری اطلاعات: شامل تضمین امنیت، ایمنی و پایداری زیرساخت‌های حوزه فناوری اطلاعات است که باعث کاهش آسیب‌پذیری‌ها و افزایش آستانه

1. Severity
2. Celerity
3. Certainly
4. Commodity

تحمل در مواجه با تهدیدات می‌شود که این امر با تأکید بر ایجاد عزم ملی از طریق فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی، هدایت راهکاری و تدوین و تصویب ضوابط و دستورالعمل‌های عمومی- تخصصی و نظام‌های هدایت‌بخش کشوری به‌منظور نهادینه نمودن رعایت اصول پدافند غیرعامل در حوزهٔ فناوری اطلاعات و نظارت بر اجرای آن با ایجاد قابلیت به‌روزرسانی میسر می‌شود. سازمان پدافند غیرعامل کشور به‌عنوان عالی‌ترین مرجع سیاست‌گذاری، برنامه‌ریزی، هدایت و کنترل راهکاری، تعیین و تصویب طرح‌ها و برنامه‌ها و خط‌مشی‌های دفاع غیرعامل کشور براساس فرامین و تدابیر فرمانده معظم کل قوا و با اتکای به خداوند متعال در پرتو تعالیم و ارزش‌های حیات‌بخش اسلام ناب محمدی (ص)، با اهتمام ویژه خود در تکیه به عزم ملی، قرار دارد.

ویژگی‌های فضای سایبری: فضای سایبری یا فضای مجازی دارای ویژگی‌هایی است که آن را از سایر فضاهای رسانه‌ای متمایز می‌سازد و امتیازات خاص و تقریباً منحصر به‌فردی دارد. از مهم‌ترین ویژگی‌های فضای سایبری، چندرسانه‌ای، به‌روزرسانی سریع، سنجش و بازخوردگیری، استفاده از فرامتن، قابلیت تعامل، توزیع افقی اطلاعات، تمرکززدایی، قابلیت دسترسی، فقدان محدودیت انتشار، فقدان سلسله‌مراتب، فقدان سانسور، تازه و دائمی بودن، آزادی از زمان و مکان، تبدیل اطلاعات، ذخیره‌سازی اطلاعات، پردازش اطلاعات، تبادل اطلاعات، تحلیل اطلاعات و انهدام اطلاعات است.

مراحل دفاع: همواره اشکال متفاوتی در برخورد با فعالیت‌های مجرمانه در یک فضای سایبر وجود دارد. در اینجا لازم است که مراحلی از دفاع ذکر شود:

جلوگیری، متوقف نمودن حملات، مدیریت حادثه، محدود کردن خرابی‌ها، تعیین آثار، نشانه‌ها و هشدارها، امن، ایمن و پایدار کردن سیستم‌ها، خاموشی و تخصیص مجدد، پشتیبانی امنیت شبکه‌های اطلاعات و ارتباطات در فضای سایبر.

کنترل امنیت اطلاعات[1]: کنترل امنیت به اقداماتی گفته می‌شود که منجر به حفاظت، مقابله، پیشگیری و یا به حداقل رساندن خطرات امنیتی است. این اقدامات را می‌توان به سه دسته تقسیم کرد.

الف- کنترل مدیریتی: کنترل مدیریتی (کنترل رویه‌ها) عبارت‌اند از سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول تأیید شده است. نمونه‌های دیگر از کنترل‌های مدیریتی عبارت‌اند از سیاست امنیتی شرکت‌های بزرگ، سیاست مدیریت رمز عبور،

1. Information Security Control

سیاست استخدام و سیاست‌های انضباطی. کنترل‌های مدیریتی پایه‌ای برای انتخاب و پیاده‌سازی کنترل‌های منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی پیاده‌سازی و ابزاری برای اعمال کنترل‌های مدیریتی هستند (Dharmapatni, 1995: 12).

ب- کنترل منطقی[1]: کنترل منطقی (کنترل فنی) استفاده از نرم‌افزار، سخت‌افزار و داده‌ها برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های رایانه‌ای است.

ج- کنترل فیزیکی[2]: کنترل فیزیکی برای حفاظت و کنترل محیط کار و تجهیزات رایانه‌ای و نحوه دسترسی به آن‌ها است که جنبه فیزیکی دارند. به‌عنوان‌مثال: درب، قفل، گرمایش و تهویه مطبوع، آژیر دود و آتش، سامانه آتش نشانی، دوربین‌های مداربسته، موانع، حصارکشی، نیروی‌های محافظ و غیره.

روش‌شناسی

این پژوهش ازنظر نوع کاربردی و ازنظر روش به شیوه توصیفی– تحلیلی گردآوری شده است. روش گردآوری اطلاعات میدانی و کتابخانه‌ای بوده و ابزار گردآوری اطلاعات پرسش‌نامه محقق‌ساخته بوده است. جامعه آماری این پژوهش متشکل از مدیران، متخصصان و کارشناسانی است که با شبکه ملی ارتباطات، تهدیدات سایبری، اصول و مبانی پدافند غیرعامل آشنایی داشته و دارای مدرک کارشناسی ارشد به بالا و حداقل ۱۰ سال سابقه کار مرتبط باشند که تعداد آن‌ها ۱۰۰ نفر برآورد شده است. حجم جامعه نمونه به‌صورت تمام‌شمار همان ۱۰۰ نفر در نظر گرفته شده است.

تجزیه‌وتحلیل

فرضیه صفر: الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری، شامل الزامات سخت‌افزاری و نرم‌افزاری نیست.

فرضیه پژوهشی: الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری، شامل الزامات سخت‌افزاری و نرم‌افزاری است.

آزمون کای۲: آزمون کای‌دو یک آزمون ناپارامتریک است که توسط فیشر ارائه شده و کار اصلی آن بررسی معناداری تفاوت بین فراوانی‌های مشاهده‌شده و مورد انتظار است. فرمول کلی کای‌دو به شکل زیر است.

f_o = فراوانی مشاهده‌شده

1. logical
2. physical

f_e = فراوانی موردانتظار

توزیع کای‌دو از توزیع نرمال به دست می‌آید. اگر متغیر X متعلق به جامعه نرمال با میانگین μ و انحراف معیار σ باشد و از این جامعه نمونه تصادفی به حجم n انتخاب شود، سپس هر یک از اعضای نمونه با استفاده از فرمول $z=\frac{x-\mu_x}{\mu_x}$ استاندارد شوند، متغیر تصادفی زیر از توزیع کای‌دو با n درجه آزادی پیروی می‌کند.

$$\varkappa^2 = {z_1}^2 + {z_2}^2 + \cdots + {z_n}^2$$

توزیع کای‌دو دارای رابطه‌ای به شکل زیر است که در آن k در جه آزادی را نشان می‌دهد و میانگین و واریانس آن به ترتیب kو ۲ k است.

$$F(x)=\frac{1}{\left(\frac{k}{1}-1\right)}*\frac{1}{2^{\frac{k}{2}}}*\chi^{\left(\frac{k}{2}-1\right)}*e^{\frac{-x}{2}}$$

$$\varkappa^2 = \sum \frac{(f_o-f_e)^2}{f_e}$$

جدول شاخص‌های موردنظر در بررسی مدیریت و امنیت اطلاعات در فضای سایبری با در نظر گرفتن اصول پدافند غیرعامل با آزمون کای۲

شاخص‌ها	خیلی زیاد		زیاد		متوسط		کم		خیلی کم		امتیاز
	تعداد	درصد	تعداد	درصد	تعداد	درصد	تعداد	درصد	تعداد	درصد	وزن ۱ تا ۵
میزان تأثیرات نفوذ شبکه‌های سازمانی در مدیریت امنیت اطلاعات	۳۷	۳۷	۱۵	۱۵	۳۱	۳۱	۱۰	۱۰	۷	۷	۳.۷۵
رضایتمندی از پاسخگو بودن اینترنت برای کاربران	۳۴	۳۴	۱۹	۱۹	۳۲	۳۲	۷	۷	۸	۸	۳.۵
میزان رضایت از مشارکت و همکاری میان ارگان‌های فعال در زمینه فناوری اطلاعات	۲۵	۲۵	۲۳	۲۳	۱۷	۱۷	۲۲	۲۲	۱۳	۱۳	۴.۵
میزان تأثیر استفاده از سیستم عامل بومی در مدیریت حملات	۳۳	۳۳	۲۷	۲۷	۲۴	۲۴	۱۰	۱۰	۶	۶	۳۳.۷۵۵

میزان تأثیر استفاده از SIEM بومی در مدیریت حملات سایبری	۳۵	۳۵	۳۸	۳۸	۱۷	۱۷	۷	۷	۳	۳	۳.۴۰
میزان تأثیر استفاده از نرم‌افزارهای امنیتی بومی در مدیریت حملات سایبری	۲۸	۲۸	۳۱	۳۱	۳۲	۳۲	۵	۵	۶	۶	۴.۵
میزان تأثیر استفاده از فایروال‌های بومی در مدیریت حملات سایبری	۲۱	۲۱	۱۲	۱۲	۴۵	۴۵	۱۴	۱۴	۸	۸	۴.۲۵
میزان تأثیر استفاده از رمزکننده‌های بومی در مدیریت حملات سایبری	۳۱	۳۱	۴۵	۴۵	۱۵	۱۵	۵	۵	۴	۴	۳.۲۵
اثربخش بودن به‌روزرسانی نرم‌افزارها در مدیریت فضای سایبر	۳۷	۳۷	۲۸	۲۸	۱۵	۱۵	۱۲	۱۲	۸	۸	۳
میزان تأثیرگذاری شناخت و مقابله با بدافزارها در امنیت فضای سایبری	۳۱	۳۱	۲۶	۲۶	۳۲	۳۲	۷	۷	۴	۴	۳.۵
مؤثر بودن حملات سایبری گذشته به مراکز حیاتی در پیشگیری از حملات	۱۴	۱۴	۲۵	۲۵	۴۰	۴۰	۱۶	۱۶	۵	۵	۳.۲۵
مؤثربودن استانداردهای بین‌المللی در تهدیدات نرم‌افزاری	۲۴	۲۴	۴۵	۴۵	۲۲	۲۲	۵	۵	۴	۴	۳.۵۰
مؤثر بودن نیروی انسانی سازمان در سامانه مدیریت اطلاعات	۲۳	۲۳	۱۲	۱۲	۲۲	۲۲	۳۲	۳۲	۱۱	۱۱	۳.۲۵
میزان اهمیت‌بخشی مدیریت و کارآمدی آن درکاهش آسیب‌پذیری در فضای سایبر	۲۱	۲۱	۲۸	۲۸	۴۲	۴۲	۴	۴	۵	۵	۲.۷۵
نقش SOC در تجهیزات سخت‌افزاری	۱۴	۱۴	۳۲	۳۲	۳۵	۳۵	۱۲	۱۲	۹	۹	۳

تأثیر تجهیزات سخت‌افزاری در مدیریت حملات سایبر	۱۳	۱۳	۲۸	۲۸	۴۲	۴۲	۱۰	۱۰	۷	۷	۴
تأثیر فناوری تجهیزات مورداستفاده در سامانه مدیریت امنیت اطلاعات	۲۷	۲۷	۳۷	۳۷	۱۸	۱۸	۴	۴	۴	۴	۲.۷۵
تأثیر استفاده از تجهیزات امنیتی سخت‌افزاری در مدیریت امنیت اطلاعات	۱۸	۱۸	۳۰	۳۰	۳۲	۳۲	۱۴	۱۴	۶	۶	۳.۵
تأثیر FIREWALLها در مدیریت حملات سایبری	۱۳	۱۳	۳۵	۳۵	۳۰	۳۰	۱۳	۱۳	۹	۹	۳.۵
میزان اثرگذاری در خصوص شناخت و استفاده از تجهیزات روزآمد در تحقق مدیریت امنیت اطلاعات	۲۱	۲۱	۳۲	۳۲	۳۲	۳۲	۸	۸	۷	۷	۲.۵۰
میزان تأثیر استفاده از انواع UTM در مدیریت حملات سایبر	۲۲	۲۲	۳۵	۳۵	۲۸	۲۸	۷	۷	۵	۵	۳
تأثیر فرایندهای سازمانی در مدیریت امنیت اطلاعات	۲۸	۲۸	۲۳	۲۳	۳۲	۳۲	۱۲	۱۲	۵	۵	۳.۲۵
میزان تأثیر سایت‌های امنیتی و حساس در دست‌یابی کارآمدتر به اطلاعات سری و محرمانه	۲۴	۲۴	۳۶	۳۶	۲۲	۲۲	۴	۴	۴	۴	۴
میزان رضایت از تناسب و هماهنگی میان اصول پدافند غیرعامل با تدابیر در نظر گرفته‌شده برای امنیت بیشتر در زمینه حفظ اطلاعات	۱۲	۱۲	۲۵	۲۵	۱۴	۱۴	۳۵	۳۵	۱۴	۱۴	۳.۵
میزان تأثیر VPN در حفظ اطلاعات و امنیت بیشتر آن	۲۶	۲۶	۳۵	۳۵	۳۲	۳۲	۱۲	۱۲	۵	۵	۴.۰۰

میزان رضایت از دسترسی راحت به اطلاعات در مواقع اضطراری	۱۸	۱۸	۲۱	۲۱	۲۰	۲۰	۳۰	۳۰	۱۱	۱۱	۴.۲۲
میزان نارضایتی از اختلال در اطلاعات موردنیاز برای اجرای عملیات	۱۲	۱۲	۱۹	۱۹	۴۸	۴۸	۱۴	۱۴	۷	۷	۳.۸۹
میزان نارضایتی از قرارگیری نامناسب عناصر نظامی امنیتی به لحاظ استقرار و آمایش پدافندی	۲۸	۲۸	۳۲	۳۲	۴۱	۴۱	۱۷	۱۷	۷	۷	۳.۵
توزیع زیرساخت‌های ارتباطی در زمان هجوم دشمن	۲۳	۲۳	۳۳	۳۳	۳۲	۳۲	۹	۹	۳	۳	۲.۵۰
رضایت از مراکز حساس و حیاتی در زمان اجرای عملیات	۱۶	۱۶	۳۰	۳۰	۲۵	۲۵	۲۰	۲۰	۹	۹	۳.۲۵

مأخذ: نگارنده

Chi-Square Test FrequenciesFARZ Asli

جدول توزیع فراوانی آزمون خی‌دو

	Observed N	Expected N	Residual
1.00	160	21.6	-20.6
2.00	370	21.6	-15.6
3.00	420	21.6	.6
4.00	3050	21.6	27.4
5.00	3800	21.6	9.4
Total	7800		

Test Statistics جدول آزمون خی‌دوی فرضیه اصلی

	FARZ ASLI
Chi-Square(a)	49.680
df	3
Asymp. Sig.	.000

داده‌های جداول فراوانی توزیع و آزمون خی‌دوی فرضیه اصلی حاکی از آن است که ارزش خی‌دوی مشاهده‌شده (49,680) از ارزش خی‌دوی بحرانی (۱۳.۲۸) در سطح P<۰/۰۱ بزرگ‌تر است، درنتیجه چنین استنباط می‌شود که فرضیه صفر با ۹۹ درصد اطمینان رد و فرضیه اصلی (پژوهشی) تأیید می‌شود؛ یعنی با ۹۹ درصد اطمینان می‌شود گفت که الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری، شامل الزامات سخت‌افزاری شامل استفاده از تجهیزات بومی همچون زیرساخت‌های بومی، ذخیره‌سازهای اطلاعات بومی، تجهیزات ارسال و دریافت بومی و الزامات نرم‌افزاری شامل استفاده از نرم‌افزارهای بومی همچون نرم‌افزارهای ارسال و دریافت فایل و اطلاعات، ضدویروس، و دیوار آتشین بوده است.

نتیجه‌گیری

منابع اطلاعاتی یک دولت جزء دارایی‌های آن است و دولت‌ها علاوه‌بر تأمین امنیت منابع اطلاعاتی خود، باید متعهد باشند که مجموعه سیاست‌هایی را برای ایمن ساختن اطلاعات زیرساختی ملی خود تنظیم کنند. این سیاست‌ها نقش مهمی در امنیت فناوری اطلاعات دارد؛ ولی بااین‌حال تناقضی وجود خواهد داشت و آن اینکه چهارچوب سیاست ملی باید قادر به افزایش سطح امنیت باشد اما قوانین ضعیف دولتی بیش از سودی که باید در پی داشته باشد، ضرر به بار خواهند آورد. فناوری به‌سرعت در حال تغییر است و تهدیدات رایانه‌ای جدید به دلیل همین تغییرات به وجود می‌آیند. درنهایت برای حفاظت از سامانه‌های امنیت اطلاعات الزاماتی با رویکرد پدافند غیرعامل وجود دارد که در دو حوزه سخت‌افزاری و نرم‌افزاری بایستی به شرح زیر قابل بهره‌برداری باشد:

برای محافظت از سامانه‌های اطلاعاتی سخت‌افزاری و نرم‌افزاری رایانه‌ای شناسایی قسمت‌های مختلف سامانه آسیب‌پذیری‌های موجود در آن ضروری است. پس از شناسایی و رفع آسیب‌پذیری‌های سیستم باید مرتباً مواظب بود که آسیب‌پذیری‌های جدید به وجود نیاید و به‌طور دوره‌ای سیستم را بررسی کرد تا از امنیت آن مطمئن شد؛ درحالی‌که هیچ‌گاه نمی‌توان صددرصد از امنیت یک سیستم مطمئن بود ولی با اقدامات زیر می‌توان تا حد بسیار بالایی امنیت و حفاظت از یک سیستم را فراهم ساخت:

۱- تهیه نقشه و راهنمای سیستم: این کار شامل شناسایی رایانه‌ها و شبکه‌های متصل و غیرمتصل به اینترنت و به خط تلفن و یا بی‌سیم، نرم‌افزارها و سیستم‌های عامل مورداستفاده نرم‌افزارهای ضدویروس و محافظ و اطلاعات و برنامه‌های حساس تجاری خواهد شد.

۲- تهیه سیاست امنیتی: این کار شامل تعریف سیاست‌های مربوط به استفاده از رایانه‌ها توسط کارکنان و روش‌های مورداستفاده در امنیت و حفاظت اطلاعات است. این سیاست

چهارچوبی را برای حفاظت از شبکه‌های رایانه‌ای و منابع اطلاعاتی موجود در آن‌ها تعیین می‌کند. این سیاست باید به‌سادگی برای مدیران و کارکنان قابل‌درک بوده و تمامی نکات و موارد مربوط به امنیت را دربرگیرد. ازجمله مطالب مهم این سیاست عبارت‌اند از:

تعریف استفاده مجاز، چگونگی احراز هویت و انتخاب کلمه رمز، مسئولیت به‌روزکردن نرم‌افزارهای موجود در هر رایانه، اقدامات لازم در هنگام بروز یک حمله و یا ویروس رایانه‌ای و مسئولیت‌های افراد در این مورد. معمولاً سیاست امنیتی در دو شکل تهیه می‌گردد. یکی به‌صورت ساده و کلی که برای عموم کارکنان قابل‌استفاده باشد و دیگری با جزئیات بیشتر که معمولاً محرمانه است و برای استفاده مدیران و کارشناسان فناوری اطلاعات و امنیت است.

۳- کاهش نقاط دسترسی و کنترل نقاط باقیمانده: این مرحله شامل بررسی نقشه سیستم و شناسایی نقاط اتصال به اینترنت و دسترسی از راه دور به‌منظور کاهش نقاط دسترسی به حداقل ممکن و کنترل نقاط باقیمانده از نظر دسترسی و ورود و خروج اطلاعات است.

۴- شناسایی نقاط ورود پنهان: شناسایی و حذف مودم‌ها و نقاط دسترسی غیرمعمول که احتمالاً از نظرها پنهان می‌ماند ولی بعضی از کارکنان آن‌ها را مورداستفاده قرار می‌دهند.

۵- نصب دیواره آتش: این سیستم برای جداسازی و محافظت سیستم داخلی از اینترنت و همچنین کنترل دسترسی به پایگاه‌های اینترنتی به‌خصوص وبگاه‌های غیرمربوط به کار نصب می‌گردد. در مواردی می‌توان رایانه‌های مشخصی را جهت استفاده از اینترنت اختصاص داد. درصورت‌نیاز تغییر درگاه‌های اتصال و آموزش کارکنان درمورد راه‌های درست دسترسی حائز اهمیت است.

۶- نصب سیستم‌های تشخیص و جلوگیری از ورود غیرمجاز[1]: این سیستم‌ها به‌مانند دزدگیر عمل کرده و ورود و دسترسی غیرمجاز به سیستم را ثبت و اطلاع می‌دهد و یا از انجام آن جلوگیری می‌کند. حتی در مواردی‌که عبور غیرمجاز از دیواره آتش انجام پذیرد با استفاده از این سیستم می‌توان آن را شناسایی و از بروز مجدد آن جلوگیری کرد. همچنین با بررسی به‌موقع لیست ثبت‌شده توسط سیستم ای‌دی‌پی و شناسایی تلاش‌های انجام‌شده برای دسترسی غیرمجاز به سیستم می‌توان از خطرات آتی جلوگیری کرد.

۷- نصب نرم‌افزارهای ضدویروس: نصب نرم‌افزارهای ضدویروس در دروازه‌های ورودی سیستم و در رایانه‌ها، احیاناً برای شناسایی و جلوگیری از ورود ویروس‌های رایانه‌ای به سیستم و مرمت

1.Intrusion detection and prevention system

سیستم‌های آلوده به ویروس ضروری است. این نرم‌افزارها باید مرتباً به‌روز درآیند تا همواره از آخرین اطلاعات مربوط به ویروس‌های رایانه‌ای استفاده گردد.

۸- بررسی پی‌درپی عملکرد سیستم و رفع اشکالات آن: این بررسی‌ها به مدیریت این امکان را می‌دهد تا با در نظر گرفتن خطرات امنیتی موجود و نیاز به انجام عملیات تجاری، ضمن رفع اشکالات شناخته‌شده سیاست و برنامه امنیتی متناسب و متوازنی را اتخاذ کند.

۹- آموزش کارکنان: کارکنان باید با توجه به نیاز آن‌ها در سطوح مختلف دربارهٔ مسائل امنیتی و حفاظت از اطلاعات رایانه‌ای آموزش‌دیده و آگاهی‌های لازم را پیدا کنند. ازجمله آموزش سیاست امنیتی شبکه از ضروریات است. اینترنت و شبکه‌های رایانه‌ای موجود در سازمان‌ها و شرکت‌ها قابلیت جست‌وجو و مبادله اطلاعات را به‌صورت بی‌سابقه امکان‌پذیر ساخته است. به‌وجودآمدن تجارت الکترونیک شرکت‌هایی را که حتی در گذشته تصور آن را هم نمی‌کردند قادر ساخته است که به عرضه خدمات و کالاهای خود در سطح جهانی بپردازند. درحالی‌که چنین ابزار قدرتمندی در امر تجارت، انقلابی ایجاد کرده است. نیاز به داشتن رایانه‌های امن و دسترسی امن به اینترنت را نیز الزام‌آور ساخته است. یک شرکت کوچک یا متوسط در مقایسه با یک شرکت بزرگ که سرمایه زیادی را در راستای امن‌کردن سیستم‌های رایانه‌ای خود به‌کاربرده است، ممکن است برای یک خرابکار اطلاعاتی هدفی به‌مراتب ساده‌تر و بهتر باشد. به‌عنوان یک مدیر شما باید از چندوچون خطراتی که دسترسی به اینترنت و شبکه رایانه‌ای شما را تهدید می‌کند اطلاع داشته باشید. شما نیازمند این هستید که وقتی را به مقوله امنیت اختصاص دهید زیرا ایجاد یک سیستم امن رایانه‌ای نیازمند صرف وقت و منابع لازم است. دقت کافی توسط مدیریت و کارشناسان فناوری اطلاعات در زمینه امنیت اطلاعات و ایجاد محیط امن رایانه‌ای به شما امکان می‌دهد تا از منافع بسیاری که اینترنت و شبکه‌های رایانه‌ای بر تجارت شما ایجاد می‌کند بهره‌مند گردید. آگاهی کامل از انواع تهدیدات و چگونگی مقابله با آن‌ها خطرات ناشی از تهدیدات را به‌مرور کمتر خواهد کرد. درک مسائل امنیتی توسط مدیران و حضور مؤثر آن‌ها در ایجاد و اجرای یک برنامه امنیت اطلاعات کارآمد و متناسب با نیازهای سازمان و با رعایت استانداردهای موجود ضروری است (Asgharian: 2004).

پیشنهادها

الف- تهیه و تکمیل نقشه و راهنمای سامانه‌های ارتباطی برای سازمان‌های دولتی و غیردولتی.

ب- تهیه سیاست‌های امنیتی ملی و نظارت بر سیاست‌های سازمان‌های دولتی و غیردولتی مرتبط با سیاست‌های ملی

ج- به‌روزرسانی نرم‌افزارهای ضدویروس و دیوار آتش بومی

د- استفاده از تجهیزات بومی مرتبط با شبکه ملی ارتباطات
ه- آموزش تخصصی و جدی به کارکنان و کاربران قسمت‌های مختلف

منابع

۱. اصلانی مقدم، مصطفی (۱۳۸۵)؛ ***رساله دکتری جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی ج.ا.ا تهران***: دانشگاه عالی دفاع ملی.

۲. انتظامی، حسین (۱۳۹۰)؛ ***رساله دکتری تأثیر فناوری اطلاعات و ارتباطات بر امنیت ملی، تهران***: دانشگاه عالی دفاع ملی.

۳. بهتاش، محمدرضا و آقابابائی محمدتقی (۱۳۹۰)؛ مفاهیم پدافند غیرعامل در مدیریت شهری با تمرکز بر شهر تهران؛ مرکز مطالعات و برنامه‌ریزی شهر تهران.

۴. حسن بیگی، ابراهیم (۱۳۸۴)؛ ***حقوق و امنیت در فضای سایبری***؛ تهران، مؤسسه ابرار محاسبه.

۵. خلیل‌پور رکن‌آبادی، علی و نورعلی‌اند (۱۳۹۱)؛ « ***تهدیدات سایبری و تأثیر آن بر امنیت ملی***» تهران: دانشگاه مالک اشتر.

۶. دوست محمدیان، حمید، فاضلی، مریم سادات (۱۳۹۲)؛ (***مهندسی پدافند غیرعامل در فناوری اطلاعات***)؛ موسسه فرهنگی هنری دیباگران تهران.

۷. زرقانی، سید هادی (۱۳۹۲)؛ ***بررسی و تحلیل جایگاه نرم در پدافند غیرعامل با تأکید بر تهدیدات اجتماعی و فرهنگی***؛ همایش سراسری پدافند غیرعامل در علوم و مهندسی دانشگاه جامع امام حسین (ع).

۸. کافی، سعید (۱۳۹۳)؛ ***رساله دکتری الزامات پدافند غیرعامل شبکه ملی ارتباطات در مقابله با تهدیدات سایبری، تهران***: دانشگاه عالی دفاع ملی.

۹. موحدی نیا، جعفر (۱۳۸۵)؛ ***مفاهیم نظری و عملی دفاع غیرعامل، تهران***: معاونت آموزش ستاد مشترک سپاه.

۱۰.ناصری، علی و نوروزی مجتبی (۱۳۸۸)؛ ***دوره‌های امنیت در فضای تبادل اطلاعات، وزارت ارتباطات و فناوری اطلاعات.***

۱۱.واحدی، مرتضی، نصراصفهانی، مجید (۱۳۹۳)؛ ***پدافند غیرعامل و امنیت در فضای سایبری،*** دانشگاه علوم و فنون فارابی، تهران.

۱۲.وزارت پست و تلگراف و تلفن، ۱۳۸۱؛ پروژه سند راهبردی توسعه فناوری و اطلاعات، تهران: وزارت پست و تلگراف و تلفن.

۱۳.الوندی، سیروس (۱۳۹۲)؛ ***پایان‌نامه کارشناسی ارشد الزامات پدافند غیرعامل در حملات سایبری،*** تهران: دانشکده علوم و فنون فارابی.

14. Dharmapatni, Ida Ayu and Tommy Firman (1995). Problems and challenges of mega-urban regions in Indonesia: the case of Jabotabek

and the Bandung metropolitan area. In The Mega-Urban Regions of Southeast Asia, T.G. McGee and Ira M. Robinson, eds. Vancouver: University of British Columbia Press, pp. 296-314.Document No. MR-1132-A, 2000.
15. lopresti tim-essex(2005) a brief history of civil defense;civil defense association 2005.