جنگ‌های سایبری[1] و مشکل یافتن منشأ آنها (مطالعه موردی؛ بدافزار استاکس نت[2])

هادی ایمانی

کارشناسی ارشد مدیریت فناوری اطلاعات، پژوهشگر دانشگاه جامع امام حسین (ع)

تهران، ایران

imani.hadi57@gmail.com

چکیده:

فناوری اطلاعات با سرعتی که توسعه می‌یابد، در حال فراگیری تمامی ابعاد زندگی می‌باشد. این فناوری فرصت‌هایی را پیش روی بشر قرار داده است ولی از طرفی تهدیدات فراوانی را نیز بوجود آورده است. از جمله این تهدیدات حملات سایبری و اطلاعاتی به زیر ساخت‌های کشور است. بدافزار استاکس نت با حمله به زیرساخت‌های صنعتی کشور به ویژه نیروگاه‌های انرژی هسته‌ای از جمله پیچیده‌ترین حملات در سالهای اخیر بوده است. سوالی که مطرح می‌شود این است که این بدافزار چه ویژگی‌هایی را داراست که برای جنگ سایبری و اطلاعاتی در نظر گرفته شده و طراحی شده است؟ همینطور منشا و انگیزه این تهاجم سایبری در قالب این بدافزار چه بوده است؟ برای جواب به این سوال به بررسی ویژگی‌ها، مشخصات و رفتار این بدافزار پرداخته شده است. برای پیدا کردن منشا جنگ سایبری و اطلاعاتی در قالب بدافزار استاکس نت بسیاری از قدرت‌های بزرگ جهان مورد سوء ظن قرار می‌گیرند ولی مشخص کردن منشا دقیق و یافتن مدارک مستند حقوقی امری مشکل است. به طوریکه این گمنامی و نبود استناد به منشاء حمله از ویژگی‌های نبرد سایبری است. نتیجه بررسی و یافته های این مقاله نشان می‌دهد که منشاء جنگ های سایبری کاملاً واضح نیست و نمی‌توان به راحتی بدان پی برد و به همین دلیل در آینده شاهد حملات و جنگ‌های اطلاعاتی و سایبری بیشتری حتی در انواع پیشرفته‌تری خواهیم بود.

کلمات کلیدی: **جنگ سایبری، جنگ اطلاعاتی[3]، بدافزار استاکس نت، گمنامی**

[1] - Cyber War
[2] - StuxNet Malware
[3] - Infomational War

مقدمه:

پیشرفت روزافزون فناوری اطلاعات و فضای سایبر منجر به تحولات گسترده در ابعاد مختلف زندگی بشر از جمله ابعاد اجتماعی، سیاسی و دفاعی و امنیتی گردیده است. زیرساخت های و شبکه های رایانه ای گسترده ای جهت برقراری ارتباطات کارا و موثرتر برای بشر فراهم آمده است. لذا عنصر اصلی این عصر را می‌فناوری اطلاعات و ارتباطات قلمداد کرد. موتور محرکه فناوری اطلاعات و فضای سایبر را رایانه‌ها می‌دانند که البته رایانه‌ها و تجهیزات سخت افزاری را باید بخش کوچکی از فناوری اطلاعات دانست. از طرفی در این عصر سایر زیرساخت های حیاتی کشور وابستگی زیادی به فناوری اطلاعات دارند. [۱]

هرچند فناوری اطلاعات و فضای سایبر به سرعت در حال فراگیر شدن اند لیکن توسعه و بهره برداری از آنها در گرو ارتباطات امن و عدم آسیب پذیری‌ها و پاسخگویی به تهدیدات می‌باشد. مسلم است که همگام با گسترش سریع فناوری اطلاعات، ابزارها و شیوه های تهاجمی و نفوذ نیز گسترش یابد.

در زمان بحران، جنگ و حتی مواقع عادی دشمن با اتکای به اطلاعات جمع آوری شده می‌تواند به زیرساخت های حیاتی و فعالیت های کلان کشور حمله کرده و یا با مخدوش کردن سیستم های اطلاعاتی و اعتبار آنها نزد افکار عمومی و ایجاد نگرانی و هراس عمومی اقدام به راه اندازی جنگ های اطلاعاتی و سایبری نماید.

ویژگی های فناوری اطلاعات جهت امکان ساماندهی و تدارک نفوذ سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده و امکان اقدام و اختلال به مهاجمان علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیر ساخت های حیاتی می‌شود، با ایجاد و برقراری ارتباط مخرب مانع از واکنش های مناسب، ایجاد تاخیر و مشکلات جدی در آنها می‌گردد. ویروس‌ها و بدافزارها می‌توانند بدون کوچکترین هشداری در شبکه های ملی و زیر ساخت های رایانه ای نفوذ کرده و با سرعت گسترش یابند و حتی فرصت اعلام هشدار را نیز از حریف سلب نمایند. [۲] از مواردی که رایانه‌های یک کشور را مورد تهدید قرار می‌دهد، بدافزارها یا همان نرم افزارهای مخرب است که مهمترین تهدید اخیر سایبری علیه ج.ا.ا. بدافزار استاکس نت می‌باشد.

در تیرماه سال ۱۳۸۹ شرکتی به نام ویروس بلاک آدا[1] اعلام کرد نرم افزاری را بر روی سیستم رایانه یکی از مشتریان ایرانی خود مشاهده و کشف کرده است. [۴] این بدافزار در سیستم های مدیریتی اسکادای زیمنس که معمولاً در کارخانه های بزرگ تولیدی و صنعتی مورد استفاده قرار می‌گیرد، فعالیت کرده و تلاش می‌کند اسرار صنعتی رایانه های این کارخانه‌ها را بر روی اینترنت بارگذاری[2] کند. استاکس نت قادر به تخریب لوله های گاز، ایجاد خلل در فعالیت‌های تاسیسات هسته ای و حتی انفجار دیگهای بخار کارخانجات مختلف است. این بدافزار توانایی نفوذ در سیستم های کنترل که توسط شرکت زیمنس آلمان در تاسیسات صنعتی و همچنین تاسیسات تامین آب شرب، چاه‌های نفت، نیروگاه های برق و هسته‌ای و دیگر تاسیسات صنعتی نصب و بکار گرفته می‌شود، را داراست. [۵]

شرکت نرم افزاری سیمانتک از معتبرترین شرکت های امنیت نرم‌افزار سوالی را اعلام کرده که چرا ایران به این اندازه تحت تاثیر آلودگی‌های بدافزار قرار دارند؟ به گفته لووی از کارشناسان ارشد این شرکت تنها می‌توان گفت افرادی که این نرم افزارهای خاص را ساخته‌اند، آن را ویژه حمله به این نقاط جغرافیایی خاص طراحی کرده‌اند. [۵]

پیچیدگی بدافزار استاکس‌نت و تمرکز فعالیت آن در ایران، گمانه‌زنی‌هایی را در مورد هدف سازندگان آن در پی داشته است. به‌نحوی که برخی، انتشار این بدافزار خطرناک را «حمله تروریستی سایبری» و هدف اصلی آن را فعالیت‌های هسته‌ای جمهوری اسلامی به‌ویژه نیروگاه اتمی بوشهر و سانتریفیوژهای تأسیسات غنی‌سازی اورانیوم نطنز عنوان کرده‌اند. [۳] اگر چه آن گونه که علی‌اکبر صالحی، رئیس وقت سازمان انرژی اتمی ایران گفت، بدافزار استاکس نت وارد سیستم اصلی نیروگاه بوشهر نشده و فقط در بعضی از لپ تاپ‌های شخصی مشاهده شده است، با این حال باید توجه داشت که ساخت و انتشار این بدافزار با یک عزم دولتی و سیاسی انجام شده و هدف آن «جنگ سایبری» است زیرا سطح بالای طراحی و دانش تخصصی‌ای که در تولید این بدافزار به کار رفته، نمی‌تواند برای یک هکر معمولی قابل دسترس باشد. [۴]

[1] - VirusBlockAda
[2] - Upload

بلافاصله کارگروه مبارزه با ویروس های صنعتی جاسوسی با عضویت وزارت ارتباطات، وزارت صنایع، سازمان پدافند غیرعامل، کمیته افتای وزارت ارتباطات و مدیران انجمن رمز ایران تشکیل شد تا به بررسی ویروسهای صنعتی با تمرکز بر بد افزار صنعتی استاکس نت و راههای پیشگیری، پاکسازی و ایمن سازی سیستمهای صنعتی آسیب پذیر از حملات امنیتی بپردازد. [۴]

از طرفی در کنفرانس مونیخ که هر ساله میعادگاه کارشناسان امنیتی و نظامی کشورهای عمده جهان است و بررسی تهدیدهای جدید امنیتی و راه‌های مقابله با آنها موضوع آن را تشکیل می‌دهد، ولفگاگ ایشنگر، رئیس کنفرانس، در توجیه برجسته‌کردن جنگ سایبری در مباحث کنفرانس، گفت که؛ استاکس‌نت نمونه بسیار قابل اعتنایی از روش‌های جدید جنگ است که در آن نه بمبی به کار می‌رود، نه تانکی به حرکت درمی‌آید و نه گلوله‌ای شلیک می‌شود، ولی در عین حال اثرات ویرانگری بر "دشمن" می‌گذارد. [۳] حال سوالی که پیش می‌آید این است که چه کشوری با چه انگیزه ای نسبت به این حمله سایبری اقدام نموده است و چه مدارک حقوقی در میان وجود دارد. در این مقاله سعی شده است تا به بررسی جنگ اطلاعاتی در قالب بدافزار استاکس نت، ویژگی های خاص این بدافزار و منشا و انگیزه مهاجمان بپردازیم.

روش تحقیق:

این تحقیق علمی براساس هدف در زمره تحقیقات نظری قرار می‌گیرد. بطوریکه جهت مراکز تصمیم ساز در زمینه مسائل امنیتی، نظامی ودانشگاهی قابل استفاده می‌باشد. روش تحقیق در این مقاله، بر اساس ماهیت روش اکتشافی و توصیفی است. ابتدا با زمینه یابی به بررسی ویژگیها و ماهیت جنگ سایبری و بدافزار استاکس نت پرداخته و سپس به پیمایش در مورد تاثیر این بد افزار بر زیر ساخت های کشور و همینطور بررسی منشاء نفوذ این بدافزار پرداخته شده است. روش گردآوری اطلاعات روش کتابخانه ای و بررسی متون می‌باشد. در این روش با استفاده از کتابها، اینترنت، روزنامه ها، مجلات، اسناد و مدارک، مطالب مرتبط مطالعه و جمع آوری میشود، سپس مطالب جمع آوری شده در عناوین پیش بینی شده قرار می‌گیرد و در نهایت نسبت به تجزیه و تحلیل و نتیجه گیری اقدام خواهد شد. این تحقیق و مقاله از نظر زمانی حال نگر و گذشته نگر است و از نظر دوره زمانی عرضی و مقطعی می‌باشد بگونه ای روند حمله این بدافزار مورد بررسی قرار گرفته شده است. در ابتدا به چیستی جنگ های سایبری می‌پردازیم.

جنگ سایبری

دگرگونی عصر (عصر اطلاعات) و زیرساخت‌های آنها مصادیق جنگ و دفاع را دچار دستخوش می‌کند. زیرساخت اطلاعاتی و زندگی اجتماعی داده‌ها و فرایند تبدیل آنها برای تصمیم‌گیری هدف نوعی عملیات به نام جنگ سایبری است. جنگ سایبری یک توانمندی استراتژیک است مانند تسلیحات هسته‌ای در زمان جنگ سرد که عامل تهدید و یا تهدیدپذیری یک کشور محسوب می‌شود. از نظر استراتژی، جنگ سایبری معتقد است به جای تسلیحات با حجم تخریب زیاد باید تسلیحات دقیق علیه نقاط حساس به کار برد و در هر جایی که از اطلاعات بهره‌برداری خاصی می‌شود اعم از سرویس‌های خدماتی عمومی، کنترل سیستم‌ها، برنامه‌ریزی سیستم‌ها و... از جمله اهداف این نوع جنگ محسوب می‌شود. [۱۰]

اگر قائل باشیم که زمین، دریا و هوا سه بعد جنگ زمینی، دریایی و هوایی هستند؛ جنگ‌های فضایی بعد چهارم جنگ هستند و بدین منوال جنگ‌های سایبری بعد پنجم جنگ در نظر گرفته می‌شود. [۶]

بر اساس بررسی‌های دانشگاه آکسفورد، بسیاری از مقامات دولتی درک درستی از حملات سایبر ندارند. بر همین اساس دولت‌ها باید احتمال انجام حملات جدی علیه زیرساخت‌های خود را کاملاً جدی بگیرند و بین سطوح مختلف تهدید و رویدادهای هکری مختلف بر اساس ویژگی‌های آن‌ها تمایز قائل شوند. [۷]

تعریف جنگ سایبری

جنگ سایبری طیف گسترده‌ای از اقدامات در زمان جنگ و صلح را شامل می‌شود. این اقدامات می‌تواند استراتژیکی، عملیاتی و تاکتیکی در حوزه‌های مختلف سیاسی، اجتماعی، فرهنگی، نظامی و... باشد. مبنای جنگ سایبری، تهدیدات اطلاعاتی به کشورها، به کسب و کارها، به افراد و اقدامات مقابله با این تهدیدات می‌باشد. در قلمرو این تهدیدات، موضوعات مختلفی چون جرائم جنایی،

تروریسم، امنیت ملی و اختلال در زیرساخت های حیاتی قرار دارند. [۸]

جنگ سایبری رقابت‌های استراتژیک، عملیاتی و تاکتیکی در زمان صلح برای ایجاد بحران، درگیری، راه‌اندازی جنگ، بین طرفین مخاصمه، دشمنان و رقبا با استفاده از سیستم‌های اطلاعاتی برای به دست گرفتن اطلاعات و ضربه به رایانه‌ها و اطلاعات آنها می‌باشد. [۱۳]

تقسیم‌بندی جنگ سایبری

در بررسی حوزه‌های راهبردی جنگ سایبری توجه به این نکته ضروری است که در تئوری‌های جنگ دیدگاه‌های مختلفی وجود دارد. این دیدگاه‌ها را به صورت زیر تقسیم می‌شوند.

۱- جنگ فرماندهی و کنترل[۱]

۲- جنگ مبتنی بر جاسوسی / هوشمندی[۲]

۳- جنگ الکترونیک[۳]

۴- جنگ روانی[۴]

۵- جنگ اطلاعات اقتصادی[۵]

۶- جنگ نفوذگری[۶]

۷- جنگ مجازی[۷] و ... [۱۱]

موارد مختلف جنگ سایبری با توجه به گستردگی و پیچیدگی نیاز به تعاریف و شرح مبسوط دارد. ما در این مقاله به دنبال جنگ بر علیه زیر ساخت‌ها در قالب ویروس استاکس نت هستیم. لذا ما را به سوی نوعی خاصی از جنگ سایبری می‌خوانیم سوق می‌دهد.

جنگ سایبری علیه زیر ساخت ها

امروزه ایجاد زیرساخت‌های اطلاعاتی[۸] به واسطهٔ پیشرفت‌های به‌وجود آمده در عرصهٔ رایانه‌ها و شبکه‌ها تسهیل شده است. سرعت، کارایی، توان و هزینهٔ پایین این سیستم‌ها این امکان را به‌وجود آورده است که بسیاری از فعالیت‌های متعارف در بخش‌های مختلف دولتی، خصوصی و نظامی در سطح کشورها و در سطح جهانی مبتنی بر این قبیل زیرساخت‌ها انجام شود. [۷] با پیشرفت زیرساخت‌های اطلاعاتی، سایر زیرساخت‌های ملی یک کشور نیز به این بسترهای پایه ارتباطی وابسته خواهد شد در نتیجه این وابستگی، فناوری اطلاعات و سیستم های اطلاعاتی در هر کشور می‌تواند به‌عنوان هدفی جدید برای نوعی از جنگ که جنگ سایبری علیه زیرساخت‌ها نامیده می‌شود واقع شود.

این جنگ ویژگی های مخصوص به خود را داراست و آن را از بقیهٔ جنگ‌ها متمایز می‌کند این است که در بقیهٔ جنگ‌ها یگان عمل کننده با استفاده از تسلیحات یگانی (سازمانی) طراحی روش جنگیدن می‌کنند و با تاکتیک خاص خودشان وارد صحنهٔ نبرد می‌شوند. در جنگ‌های سایبری تاکتیک در تولید سلاح نهفته است و در هر نوع سلاحی که توسط برنامه‌نویس کامپیوتری تولید می‌شود (اعم از ویروس، کرم، اسب‌تروا و...) تاکتیک جنگ همان عملکرد سلاح است که به عنوان الگوریتم برنامه استفاده می‌شود. [۱۲]

جنگ سایبری در ساده‌ترین سطح خود به معنی بکارگیری رایانه‌ها برای حمله به زیرساخت‌های اطلاعاتی دشمن، در عین حفاظت از زیرساخت‌های اطلاعاتی خودی است و تهدیدات جنگ سایبری می‌تواند دامنگیر بخش‌های مختلف خصوصی و دولتی در هر کشور شود. سرقت اطلاعات استراتژیک، اقتصادی، نظامی و... یا تخریب و از کار انداختن سرویس‌ها و خدمات عمومی یا خصوصی می‌تواند نمونه‌ای از نتایج جنگ سایبری باشد. [۱۰]

جنگ سایبری را می‌توان به صورت کلی تحت عنوان:

حمله عمدی به زیرساخت‌های اطلاعاتی دشمن از طریق استفاده از تکنیک‌های نفوذگری به رایانه‌ها در عین جلوگیری کامل (یا مشکل کردن) از انجام اقدامات مشابه از طرف دشمن تعریف نمود. [۲]

این‌گونه حملات شامل موارد ذیل است:

۱- بهره‌برداری از اطلاعات

۲- جلوگیری از ارائهٔ سرویس

۳- دستکاری

۴- تخریب

۵- حذف داده‌ها [۱۱]

---

1 - Command and Control Warfar (C2W)
2 - Infelligence Based Warfare (IBW)
3 - Electronic Warfarer (EW)
4 - Psychological Warfare (PSYW)
5 - Economic Information Warfare (EIW)
6 - Hacker warfare (HW)
7 - Virtual Warfare (VW)
8 - Information Infrastructure

فضای جنگ[1] در جنگ سایبری، سرویس‌ها و شبکه‌های زیرساخت اطلاعاتی در سطوح جهانی، ملی و دفاعی است. اینترنت، شبکهٔ عمومی تلفن، سرویس‌های برخط[2]، شبکه‌های عمومی داده، شبکه‌های ماهواره‌ای، شبکه‌های رادیویی و تلویزیونی و شبکه‌هایی از این دست، این فضا را تشکیل می‌دهد. کلیهٔ عناصر و اجزای مورد استفاده در زیرساخت‌های اطلاعاتی شامل رایانه ها، اجزای شبکه، دیسک‌های فشرده، دوربین‌ها، کابل‌ها، صفحه کلید، تلفن، دستگاه‌های فاکس، تلویزیون، پرینتر و... عناصر شرکت‌کننده در جنگ اطلاعات می‌باشند. تسلیحات مورد استفاده در این جنگ بدافزارها هستند و عبارتند از: ویروس‌ها، کرم‌ها، باکتری‌ها، اسب‌های تروا و .... [۱۰]

بدافزار استاکس نت:

در ۲۶ سپتامبر سال ۲۰۰۹ میلادی مسئولان نیروگاه اتمی بوشهر از ویروسی شدن سیستم‌های نیروگاه سخن گفتند، اما تاکید کردند، این موضوع موجب از کار افتادن کامل سیستم‌های رایانه ای نیروگاه نشده است. [۴] پس از آن یک پایگاه اطلاع رسانی روسی به نقل از "یوگنی کاسپرسکی"، کارشناس روس و یکی از معروف‌ترین دانشمندان علوم رایانه ای جهان اعلام کرد که دنیا وارد عرصه جدیدی از جنگ‌ها شده که تسلیحات به کار رفته در آن ویروس‌ها هستند و به این ترتیب اعلام کرد که قرن بیست و یک بیش از هر چیز با اصطلاحات و واژه‌هایی همچون "تروریسم الکترونیکی" و "سلاح الکترونیکی" و "جنگ‌های الکترونیکی" مواجه خواهد بود. [۹]

نمودار ۱. مشخصات عمومی بدافزار استاکس نت [۳]

مشخصات ویروسی که واحدهای صنعتی را آلوده کرده است	
نام ویروس	استاکسنت
تعداد کامپیوترهای آلوده شده	۱۵ تا ۲۰ هزار دستگاه
نقاط هدف	واحدهای صنعتی بزرگ
سیستم های مورد هدف	نرم افزار مدیریت سیستم کنترل زیمنس
کشورهای مورد هدف	ایران، هند و اندونزی
اولین مورد کشف شده	ایران
احتمالات دلایل انتشار	جاسوسی صنعتی، تروریسم صنعتی، نارضایتی کارکنان
عملکرد	ربایش و انتشار اطلاعات محرمانه صنعتی
شکل گسترش	از طریق پورت USB و اینترنت
میزان خطرپذیری	بسیار بالا (برای واحدهای صنعتی)

بدافزار استاکس‌نت پیشرفته‌ترین سلاح سایبری[3] است که تاکنون تاکنون ساخته شده است. معاینات این کرم نشان می‌دهد که آن موشکی سایبری[4] است که برای نفوذ در سیستم‌های امنیتی پیشرفته طراحی شده است. این موشک سایبری مجهز به کلاهکی است که نشانه‌روی شده و کنترل سیستم‌های سانتریفیوژ در مرکز فرآوری اورانیوم نطنز را در دست می‌گیرد و کلاهک دومی دارد که توربین عظیم رآکتور بوشهر را هدف می‌گیرد. [۹]

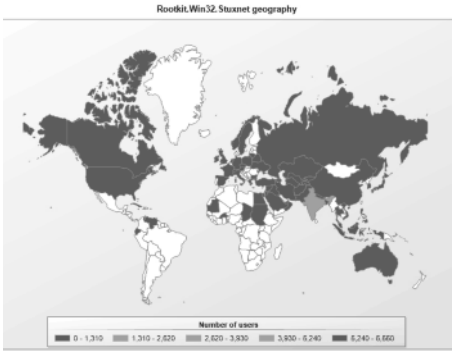
دبیر شورای فناوری اطلاعات وزارت صنایع و معادن از شناسایی ۳۰ هزار آی پی[5] صنعتی آلوده به بدافزار جاسوس "استاکس نت" نت" خبر داده و اعلام کرده که هدف گیری این بدافزار در راستای جنگ سایبری علیه ایران است و این بدافزار، اطلاعات مربوط به خطوط تولید را به خارج از کشور منتقل می‌کند. نمی توان بر روی اطلاعات قیمت گذاشت اما خسارت خیلی جدی که باعث خرابی و از کاراندازی سیستمها شود گزارش نشده اما قطعا باید به صورت کامل این بدافزار پاک سازی شود. [۴]

الیاس لووی مدیر ارشد فنی بخش پاسخگویی ایمنی سیمانتک عقیده دارد این بدافزار از ماه ژانویه سال ۲۰۰۹ میان رایانه‌ها در گردش بوده است. این بدافزار به دنبال سیستم های مدیریتی اسکادا زیمنس که معمولاً در کارخانه های بزرگ تولیدی و صنعتی مورد استفاده قرار می‌گیرد، است و تلاش می‌کند اسرار صنعتی رایانه های این کارخانه‌ها را بر روی اینترنت بارگذاری کند. اسکادا در کارخانه‌های تولیدی، نیروگاه‌های برق، تصفیه‌خانه‌های آب، صنایع نفت و گاز و برخی از آزمایشگاه های پیشرفته بخصوص انرژی هسته ای استفاده می‌شود. [۵]

نسخه ابتدایی استاکس نت نخستین بار یک و نیم سال پیش از سوی یک شرکت کوچک امنیتی در بلاروس گزارش شد و یک ماه بعد از آن نیز تایید شد که این بدافزار در کل هدف قرار دادن سیستمهای ویندوز در مدیریت سیستمهای کنترل صنعتی بزرگ است اما شرکتهای معروف دنیا که علیه بدافزارها کار می‌کنند در مورد این بدافزار که آن زمان از آسیب پذیری های ساده تری استفاده می‌کرد در مورد آن اطلاع رسانی عمومی نکرده و اقدامی خاصی در این باره انجام ندادند. متخصصان امنیتی معتقدند استاکس نت حمله ای برنامه ریزی شده به سوی مناطق صنعتی

[1] - Battle Space
[2] - On - Line
[3] - Cyber weapn
[4] - Cyber missile
[5] - IP

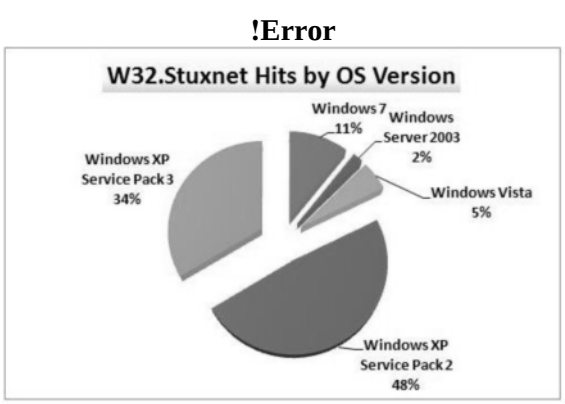
در کشورهایی خاص است. حمله ای که ۶۰ درصد آمار جهانی آن به ایران اختصاص دارد. بر اساس محاسبات سیمانتک ساخت چنین بدافزاری به گروهی با پشتیبانی مالی و اطلاعاتی قوی متشکل از حداقل ۵ تا ۱۰ نفر خبره نیاز دارد که دست کم ۶ ماه را صرف ساخت آن کرده باشند. [۵]



شکل ۱. جغرافیای آلودگی استاکس نت [۵]

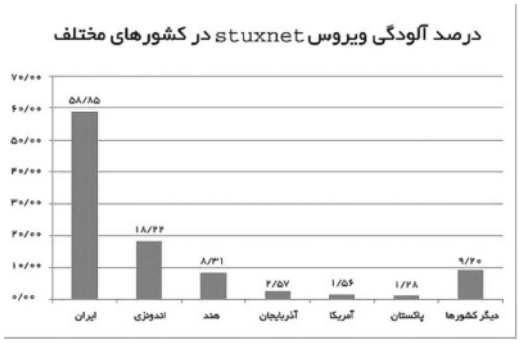
به همین دلیل به نظر می‌رسد این بدافزار با اهدافی خاص نیروگاههای اتمی ایران را مورد هدف قرار داده است. استاکس می‌تواند به طور همزمان از چهار آسیب پذیری برای دسترسی به شبکه های رایانه ای استفاده کند و به اعتقاد کارشناسان پیش از این دیده نشده که یک بدافزار به طور همزمان از چهار آسیب پذیری استفاده کند. ساماندهی و پیچیدگی این بدافزار بحدی قابل توجه و اعجاب انگیز است که محققان معتقدند که کسانی که پشت این بدافزار قرار دارند، قصد دارند به تمام دارایی های رقیب یا شرکتهای رقیب خود دست یابد. [۳] همچنین محققان امنیتی براین باورند که تیمی متشکل از افرادی با انواع تخصصها و پیش زمینه های صنعتی و فناوری اطلاعات این بدافزار را ایجاد کرده و هدایت می‌کنند. کارشناسان معتقدند که سطح بالایی از تخصص فنی در نوشتن این بدافزار مورد استفاده قرارگرفته است و به همین دلیل انگیزه عادی یا کسب درآمد در نوشتن آن مطرح نبوده است. به همین دلیل است که گفته می‌شود یک سازمان یا یک دولت متخاصم علیه ایران ممکن است دست به این اقدام سایبری زده باشد. بدافزار مذکور با سوء استفاده از یک حفره امنیتی در ویندوز گسترش پیدا می‌کند و به دنبال سیستم هایی است که از نرم افزار ویندوز اسکادا[1] که متعلق به زیمنس است، استفاده می‌کنند. نرم افزار مذکور معمولاً توسط سازمان های مرتبط با زیرساخت های حیاتی مورد استفاده قرار می‌گیرد. شکل زیر آسیب پذیری نسخه های ویندوز را نسبت به بدافزار نشان می‌دهد. [۵]

نمودار ۲. آلودگی سیستم عاملها توسط استاکس نت [۵]



بنا بر اطلاعات ارائه شده توسط سایمانتک، استاکس نت که هدف آن شرکت‌ها و سازمان های مربوط زیرساخت های حیاتی هستند، نه تنها به سرقت اطلاعات می‌پردازد، بلکه یک در پشتی[2] را نیز بر روی سیستم قربانی قرار می‌دهد تا بتواند از راه دور و به طور مخفیانه کنترل عملیات زیرساخت های مذکور را در اختیار گیرد. بدافزار استاکس نت، شرکت های مربوط به سیستم های کنترل صنعتی در سراسر جهان را آلوده ساخته است، با این وجود بنا بر گزارش های دریافت شده، بیشتر آلودگی‌ها در ایران و هند مشاهده شده است. همچنین بدافزار مذکور توانسته است خساراتی را به صنعت انرژی در ایالات متحده آمریکا وارد سازد. [۵]

نمودار ۳. درصد آلودگی استاکس نت در کشورهای مختلف [۳]



[1] - WinCC Scada

[2] - back door

رفتار و عملکرد بدافزار استاکس نت:

مرکز مدیریت امداد و هماهنگی عملیاتی رخدادهای رایانه‌ای که زیر نظر وزارت فناوری اطلاعات و ارتباطات فعالیت می‌کند به‌نقل از یکی از مدیران فنی سایمانتک به نام اریک چین گزارش داده است که این بدافزار، سیستم‌هایی را هدف قرار داده که دارای یک مبدل فرکانس هستند که نوعی دستگاه برای کنترل سرعت موتور است. بدافزار استاکس‌نت به‌دنبال مبدل‌هایی از یک شرکت در تهران بوده است. او ادامه داد: استاکس‌نت روی سیستم قربانی به‌دنبال این دستگاه‌ها می‌گردد و فرکانسی را که دستگاه‌های مذکور با آن کار می‌کنند، شناسایی کرده و به‌دنبال بازه‌ای از ۸۰۰ تا ۱۲۰۰ هرتز می‌گردد. در صورتی که نگاهی به برنامه‌های سیستم‌های کنترل صنعتی بیندازید، متوجه می‌شوید که تعداد کمی از آنها از مبدل‌هایی با سرعت مذکور استفاده می‌کنند؛ برنامه‌های مذکور واقعاً محدود هستند. [۵]

این بدافزار از نام کاربری و کلمه عبوری که در نرم افزار زیمنس به صورت رمز سخت[1] وجود دارد، سوءاستفاده می‌کند. اصلی‌ترین راه انتشار بدافزار استاکس نت، استفاده از حافظه‌های قابل حمل است. در این روش، بدافزار دارای یک شمارشگر است و تعداد دفعاتی که یک حافظه می‌تواند باعث آلودگی شود، به سه دفعه محدود شده است. این محدودیت نشان می‌دهد که ویروس‌نویسان نمی‌خواستند که دامنه آلودگی گسترش یابد و تاکید داشته‌اند که انتشار آلودگی فقط محدود به چند کامپیوتر اطراف آلودگی اولیه باشد. همچنین در روش انتشار از طریق شبکه محلی، یک آلودگی فقط در سه هفته اول به دیگر ماشین‌های داخل شبکه، انتشار می‌یافت و پس از آن، هیچگونه فعالیتی برای شیوع و انتشار خود انجام نمی‌داد. آن چه در مورد این بدافزار بیش از هر چیز مشخص بود، شیوه‌ای است که بدافزار به وسیله آن این عملکردها را مخفی می‌کرد. عملکرهای ویندوز معمولاً زمانی که لازم باشد از یک فایل دی ال ال[2] ذخیره شده روی هارد دیسک، بارگذاری می‌شوند. بنابراین انجام این کار با استفاده از فایل‌های مخرب، نشانه‌ای را به دست آنتی‌ویروس می‌دهد. استاکس‌نت فایل دی ال ال رمزگشایی شده خود را، به جای هارد دیسک، تنها در حافظه رم ذخیره و آن را به عنوان یک فایل مجازی با اسمی که به شکل خاص تعیین شده بود، ایجاد می‌کرد. این بدافزار سپس رابط بین سیستم عامل و برنامه‌های نصب شده روی ویندوز را به گونه‌ای برنامه‌ریزی می‌کرد که هر گاه برنامه‌ای بخواهد عملکردی را از یک لایبرری با آن نام خاص بارگذاری کند، به جای هارد دیسک درون حافظه، رم آن را بیابد. استاکس‌نت در اصل، نسل کاملاً جدیدی از فایل‌های مخفی را ایجاد کرده بود که روی هارد دیسک ذخیره نمی‌شدند و به همین دلیل نیز یافتن آن‌ها تقریباً غیر ممکن بود. [۹]

کارشناسان امنیتی تشخیص دادند که هر گاه استاکس‌نت رایانه‌ای را آلوده می‌کند، "به خانه زنگ می‌زند" تا اطلاعاتی را در مورد رایانه آلوده شده گزارش دهد. این اطلاعات شامل آدرس‌های داخلی و خارجی آی‌پی، نام رایانه، سیستم عامل و نسخه آن بود و همچنین این که آیا نرم‌افزار "زیمنس سیماتیک وین‌سی‌سی استپ ۷" یا به شکل خلاصه "استپ ۷"، بر روی این رایانه نصب است یا خیر. سرورهای کنترل و فرماندهی به مهاجم‌ها اجازه می‌دادند تا استاکس‌نت را روی رایانه‌های آلوده به‌روزرسانی کنند و عملکردهای جدید و یا حتی فایل‌های مخرب بیشتری را در رایانه آلوده به این بدافزار اضافه کنند. ظاهراً این اقدام با هدف ایجاد تغییرات در سرعت چرخش سانتریفیوژ صورت گرفته است بدین صورت که اول این سرعت افزایش و سپس کاهش یابد تا نوعی اختلال یا تغییر ناگهانی ایجاد گردد و سانتریفیوژها از کار بیفتد. [۹]

نمودار ۴. مشخصات فنی بد افزار استاکس نت [۵]

نام	W32.StuxNet
سطح ریسک	کم (۲ از ۵)
تاریخ کشف	July 13, 2010
آخرین بروز رسانی	September 17, 2010 8:53:13 AM
شناخته شده با نام های دیگر	Troj/Stuxnet-A [Sophos], W32/Stuxnet-B [Sophos], W32.Temphid [Symantec], WORM_STUXNET.A [Trend], Win32/Stuxnet.B [Computer Associates], Trojan-Dropper:W32/Stuxnet [F-Secure], Stuxnet [McAfee], W32/Stuxnet.A [Norman]
نوع بدافزار	کرم
روش انتقال	چند گونه ای
سیستم های تحت تاثیر	Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000
نام امضاهای ثبت شده در پایگاه داده	W32.Stuxnet

[1] - hard-coded
[2] - DLL

ضد ویروسها	
نام شناخته شده برای ضدویروسها (تشخیص هوشمند)	W32.Stuxnet!lnk
نام ثبت شده در پایگاه داده نرم افزارهای تشخیص نفوذ	HTTP W32 Stuxnet CC Activity HTTP W32 Stuxnet CC Activity 1
ارزیابی ریسک	خطر میزان خطر: سطح کم آلودگی:سطح متوسط توزیع جغرافیای:سطح کم کاهش ریسک: آسان حذف :آسان سطح آسیب پذیری سطح آسیب پذیری:متوسط سطح توزیع در سیستمها: متوسط سطح توزیع در درایوهای به اشتراک گذاشته شده:زیاد سطح توزیع در حافظه های قابل حمل:زیاد سطح توزیع در سیستمهای به روز نشده: زیاد
منبع	CVE-2010-2568
توضیحات	این ویروس اولین بار در july 2010 توسط Symantec شناسای شد و به اسم W32.TEMPHID نام گذاری شد سپس به استاکس نت تغییر نام داد. به همین دلیل در تاریخ 19 july 2010 یا ما قبل آن این کرم به نام W32.TEMPHID شناخته شده است. اهداف استاکس نت در سیستم های کنترل صنعتی به منظور تحت کنترل گرفتن از تجهیزات صنعتی مانند نیروگاهها بوده در حالی که انگیزه های دقیق مهاجم برای انجام این کار مشخص نیستند، بعضی بر این باورند این کرم برای جاسوسی صنعتی بوده است. هویت حمله کنندگان نیز ناشناخته است ، اما به نظر می‌رسد آنها به مهارت و اطلاعات حساس صنعتی دسترسی داشته اند. و همچنین این ویروس از۴ نقطه ضعف منتشر نشده که اصطلاحا Zero Day گفته می‌شود استفاده می‌کند که در نوع خود بی نظیراست.
روش آلوده سازی	استاکس نت اولین بدافزار مخربی بوده که از نقطه ظعف Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) سواستفاده کرده تا بتوان خود را انتشار دهد. این کرم یک نمونه از خود را توسط این نقطه ضعف در درایوهای یواس بی کپی می‌کند. وقتی دیسکهای قابل حمل به سیستم متصل می‌شوند و توسط برنامه های ویندوزی که آیکون‌ها را نمایش می‌دهند مانند Windows Explorer باز شوند می‌توانند سیستم راآلوده سازند.
کاربردپذیری	استاکس نت در همه کشورهای جهان و به خصوص ایران گسترش پیدا کرده است که هدف آن ایجاد اختلال در شرکت‌ها و سازمان‌های مرتبط با زیرساخت‌های حیاتی

همچون نیروگاه‌ها است. بدافزار مذکور با سوءاستفاده از یک حفره امنیتی در ویندوز گسترش پیدا می کند و به دنبال سیستم هایی است که از نرم افزارWinCC Scada که متعلق به زیمنس است، استفاده می کنند. نرم افزار مذکور معمولاً توسط سازمان‌های مرتبط با زیرساخت‌های حیاتی مورد استفاده قرار می گیرد.

کرم استاکس نت ، شرکت‌های مربوط به سیستم‌های کنترل صنعتی در سراسر جهان را آلوده ساخته است، با این وجود بنا بر گزارش‌های دریافت شده، بیشتر آلودگی در ایران مشاهده شده است. استاکس نت با سوءاستفاده از یک حفره امنیتی در ویندوز، خود را منتشر می سازد. حفره امنیتی مذکور که در همه نسخه‌های ویندوز وجود دارد مربوط به پردازش فایل‌های میان بر با پسوند lnk.است. این ویروس از طریق درایوهای یو اس بی، سیستم‌های قربانی را آلوده می سازد، با این وجود بنا بر اطلاعات ارائه شده توسط مایکروسافت، این ویروس همچنین می تواند در یک وب سایت، اشتراک‌های شبکه از راه دور یا در فایل‌های ورد نیز مخفی شده و از این طرق به گسترش آلودگی بپردازد

منشا بدافزار استاکس نت:

نفوذ چنین بدافزارهای پیچیده‌ای جز با حمایت‌های دولت‌ها و حکومت‌ها امکان پذیر نبوده و اطلاعات به دست آمده نشان می‌دهد، ایجاد کنندگان چنین ویروسی آشنایی کامل و جامعی به سیستم عملکرد شرکت آلمانی "زیمنس" داشته و به این ترتیب بدافزار "استاکس نت" توانسته وارد سیستم‌های الکترونیکی و رایانه ای نیروگاه بوشهر شود. لازم است به سناریو های مختلف بپردازیم. اولین کشوری که به ذهن می‌آید، روسیه است. آیا گرفتن انتقام پرونده «فرول» می‌تواند انگیزه این کشور باشد؟ کمی دور از ذهن به نظر می‌رسد. شاید روسیه به خاطر کاربردهای امنیتی استاکس نت اولیه و جدید، به این بدافزار علاقه‌مند شده باشد. کاربرد و کارکرد این بدافزار رایانه ای می‌تواند به روسیه کمک کند تا امنیت تجهیزات هسته ای خود را افزایش دهد و از برهم خوردن نظم سامانه های ارتباطی خود در حین انجام عملیات نظامی، محافظت کند. روسیه در سال ۲۰۰۸ و در کشمکش‌های سیاسی با گرجستان، از تجهیزات جنگ سایبری خود علیه دولت، غیرنظامیان و تجهیزات اینترنتی ارتش استفاده کرد. [۳]

از طرفی چین در حال سازماندهی تجهیزات جنگ سایبری برای رسیدن به «شبکه ای منسجم از جنگ افزارهای الکترونیک»

است؛ شبکه ای که توانایی هدف قرار دادن غیرنظامیان آمریکایی و زیرساخت‌های نظامی را دارند، از ماهواره گرفته تا چراغ‌های خطر راهنمایی و رانندگی. برای مثال حمله یادشده به شرکت لاکهید با استفاده از زیرساخت‌ها و امکانات اینترنتی چین انجام شد، بدون آن که بتوان ثابت کرد که واقعاً دولت چین هم در آن نقشی داشته است. یک منبع هندی، چین را به عنوان عامل طراحی و راه اندازی بدافزار رایانه ای استاکس نت معرفی کرد. تایمز هند در مطلب خود که با عنوان "چین با استاکس نت به هند ضربه می‌زند" چاپ شده می‌نویسد: استاکس نت که گفته می‌شود برای نفوذ در تاسیسات هسته ای ایران طراحی شده ممکن است در گام اول برای نفوذ در هند و ضربه زدن به تاسیسات هند ساخته شده باشد و غیر از چین کسی دیگری عامل آن نباشد. جفری کار از متخصصان جنگ سایبری آمریکا در این باره می‌گوید: بیش از هر کشوری احتمال دست داشتن چین در طراحی این کرم رایانه ای محتمل است. هند با ثبت شش هزار مورد نفوذ استاکس نت در رایانه های دولتی یکی از قربانیان بزرگ استاکس نت محسوب می‌شود. «جفری کار» در مقاله‌اش با عنوان «اژدها، ببر، مروارید و کیک زرد»، به چهار سناریو در مورد ارتباط استاکس‌نت و چین پرداخت. این متخصص امنیت سایبری توضیح می‌دهد که چگونه در تحقیقاتش رابطهٔ میان شرکت فنلاندی وکن[1] و ری‌یل‌تاک[2] و این بدافزار را کشف کرده است. به ادعای چین برای طراحی «استاکس‌نت» به اطلاعات شرکت‌هایی احتیاج داشته که از قضا به رغم اروپایی بودن، مراکزی در تایوان و چین نیز دارند. [۴]

ریچارد پرل معاون پیشین وزارت دفاع آمریکا به تولید بدافزار استاکس‌نت توسط رژیم صهیونیستی و شکست این برنامه در توقف کار تأسیسات هسته‌ای ایران اذعان دارد. [۳]

پیشینه تولید بدافزار استاکس نت را سال ۲۰۰۹ می‌دانند بطوریکه طرح اولیه تولید این ویروس را «مائیر داگان»، رئیس موساد، به «بنیامین نتانیاهو» ارائه داد و ضمناً هشدار داده بود که احتمالاً کنترل این بدافزار پس از انتشار کار هزینه بر و سختی خواهد بود و ممکن است به اطلاعات طبقه بندی شده آمریکا درباره ایران نیز صدمه بزند که «نتانیاهو» با وجود این احتمال خطرناک، دستور حمایت مالی از تولید از این بدافزار را می‌دهد. همچنین قابلیت خاص "استاکس نت" که از برخی رمز عبورهای زیمنس آلمان برای ایجاد ریموت استفاده می‌کند، همکاری متخصصان این تیم را که بیشتر آنها را افراد یهودی تشکیل می‌دهند را به حقیقتی قابل انکار تبدیل می‌کند. [۳]

با تجزیه و تحلیل برنامه‌نویسی استاکس‌نت و رمزگشایی کد آن، لیام مارچو[3] مدیر عملیاتی شرکت سیمنتک[4] دریافت که به احتمال زیاد متهم پشت پرده حمله به ایران، اسرائیل است. ترت پست[5] نیز از کارشناسان امنیتی در گزارشی می‌نویسد: شواهدی وجود دارد که نشان می‌دهد سازمان اطلاعات اسرائیل سازنده بدافزار استاکس‌نت است، لیام مارچو برنامه نویس آنتی ویروس موردی را ذکر می‌کند که محققان در کد این ویروس تاریخ ۹ می ۱۹۷۹ را کشف کرده‌اند که تاریخی است که حبیب اقانیان یهودی برجسته ایرانی، مدت کوتاهی پس از انقلاب ایران اعدام شد. تعدادی از کارشناسانی در انبوه کدهای نوشته شده برای کرم استاکس‌نت، چند علامت پیدا کردند. اولین علامت در کدها کلمه «مایرتوس» بود. این کلمه در زبان عبری، نشان از درختی ویژه دارد. هم‌چنین در کدها کلمه «استر» وجود دارد. او دختری یهودی بوده که همسر اردشیر، پادشاه ایران شد. استر از موقعیت خود استفاده کرده و قوم یهود را از قتل‌عام نجات می‌دهد. [۳]

نیویورک تایمز گزارشی دارد که کارشناسان اتمی آمریکایی و متخصصان زیمنس در سال ۲۰۰۸ طی طرحی تحقیقاتی با هدف جلوگیری از حملات احتمالی سایبری به «آزمایش ملی آیداهو» که از مراکز اتمی بزرگ ایالات متحده است، به دقت نقاط ضعف سیستم کنترل صنعتی ساخت زیمنس را بررسی کرده بودند. [۹]

ریچارد سیل در کتاب جنگ‌های پنهان کلینتون تشدید حملات سایبری اسرائیل و آمریکا علیه برنامه هسته ای ایران را مورد بررسی قرار داده است. به نظر می‌رسد که ساخت یک بدافزار جدید که طرح اولیه آن از بدافزار رایانه ای استاکس نت برداشته شده است، در دستور کار قرار گرفته است. به گفته مسئولان اطلاعاتی سابق و کنونی دولت آمریکا، رهبران ۳ شرکت نرم افزاری بزرگ، سرگئی برین از شرکت گوگل، استیو بالمر از شرکت مایکروسافت و لری الیسون از شرکت اوراکل با زبده‌ترین متخصصان حوزه جنگ سایبری اسرائیل همکاری کرده و

[1] - Vacon
[2] - RealTek
[3] - Liam O'Murchu
[4] - Symantec
[5] - Threat Post

توانسته‌اند نسخه جدیدی از بدافزار رایانه ای استاکس نت را تولید کنند. نوح شیتمن از کارشناسان اندیشکده بروکینگز در گزارشی فاش کرد که آمریکا و متحدانش برای تصویب قانون امنیت سایبری، نرم افزار مخرب استاکس‌نت را منحصراً برای حمله به رآکتور اتمی بوشهر طراحی کرده اند. [۶]

نتیجه‌گیری:

می توان چنین نتیجه‌گیری کرد که قدرت‌های جهانی امید بسیاری به استاکس‌نت داشتند و جنگ سایبری را بسیار کم هزینه‌تر از هر ابزار دیگری برای توقف برنامهٔ هسته‌ای ایران می‌دانند. پیچیدگی بدافزار استاکس‌نت و تمرکز فعالیت آن در ایران، گمانه‌زنی‌هایی را در مورد هدف سازندگان آن در پی داشته است. به‌نحوی که برخی، انتشار این بدافزار خطرناک را حمله و جنگ سایبری و هدف اصلی آن را فعالیت‌های هسته‌ای جمهوری اسلامی به‌ویژه نیروگاه اتمی بوشهر و سانتریفیوژهای تأسیسات غنی‌سازی اورانیوم نطنز عنوان کرده‌اند. بررسی های انجام شده بر روی استاکس نت نشان می‌دهد که این بدافزار با بیشترین احتمال کار آمریکا و اسرائیل می‌باشد. سناریوی پیش رو بدین صورت است که آمریکایی‌ها با هماهنگی رسانه های گروهی اروپا، وظیفه اطلاع رسانی درباره این بدافزار را انجام دادند و اسرائیل با تولید این بدافزار و ارسال آن، این جنگ سایبری را به راه انداختند. ضمن این که اثبات دقیق همکاری سایر دولت‌ها در حملات سایبری هم یکی از سناریوهای احتمالی می‌باشد. در حالی که دلایل متقنی برای ارائه به دادگاه های بین المللی را نمی‌توان ارائه داد.

با توجه به بودجه های کلان دولت‌ها و برنامه ریزی‌ها و تدارکات فراوان در کشورها، از این به بعد باید منتظر حملات سایبری بیشتری را در کشور باشیم و به موازات آن حملات سایبری برنامه ریزی شده ای در دنیا را نیز شاهد هستیم که توجهات و نگاه های فراوانی را به سمت خود میکشاند. بطوریکه هزینه پایین ورود، ناشناسی و عدم تقارن در آسیب پذیری است که بازیگران را قادر در بکارگیری حملات و تهاجمات در فضای سایبر می‌نماید و این امر نسبت به سایر حوزه های سنتی تر سیاست بین الملل نمود بیشتری دارد.

مراجع:

[۱] حسن بیگی، ابراهیم، **حقوق و امنیت در فضای سایبر**، تهران، انتشارات دانشگاه عالی دفاع ملی، ۱۳۸۸.

[۲] والتز، ادوارد، **جنگ اطلاعات- اصول و عملیات**، مترجمین؛ اکبر رنجبر و همکاران، تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی- طرح فراسازمانی فاوا نیروهای مسلح، ۱۳۸۵.

[۳] خبرگزاری فارس

[۴] خبرگزاری مهر

[۵] سایت سیمانتک Symantic.com

[6] Joseph S. Nye, JR, *Cyber Power*, Harvard Kennedy School: Belfer Center For science and International Affairs, May 2010

[7] Turbon, Efrain, *Information technology for management transforming organization in the digital economy*, 5th, John Willey & sons Inc, 2006.

[8] United States Air Force, *Joint Doctrine for Information Operation*, Joint Pub 3-13, October 1998.

[9] [CERT] Computer Emergency Response Team, http://www.cert.org/

[10] R. E. Overill. *Information Warfare: Battles in Cyberpace*, Computing & Control Engineering Journal, Vol. 12, no. 3, pp. 125-128, 2001.

[11] G. L. Kovacich, *Information Warfare and the Information Systems Security Professional*, Computers & security, vol. 16,no. 1,pp. 14-24, 1997.

[12] J. Kumagai, *The Web As Weapon [Cyber Warfare]*, IEEE Spectrum, vol. 38,no. 1, pp. 118-121, 2001.

[13] Libicki, M.C, *What is Information Warfare?* Washington D.C, National Defence University, 1995.