تاریخ دریافت: ۱۳۹۵/۰۳/۲۵
تاریخ پذیرش: ۱۳۹۵/۰۷/۱۱

فصلنامه دانش امنیتی
سال اول * شماره چهارم * زمستان ۱۳۹۶

بررسی تهدیدات فضای سایبری و تأثیرات آن بر امنیت و اقتدار کشور

علی جلالی[۱]
احمد سعادتمند[۲]

چکیده

فضای سایبری با رشد چشمگیر و بی‌وقفه خود به یکی از عرصه‌های مهم زندگی امروزی انسان تبدیل‌شده است. تحولات در این حوزه آن‌چنان سریع پیش می‌روند که پیش‌بینی و تحلیل جامع تأثیرات آن بر افراد و اجتماع را غیرممکن کرده است. امروزه دیگر نمی‌توان امنیت، اقتدار و قدرت نرم کشوری را بدون احتساب قدرت فنی و عملیاتی آن در حوزه سایبری ارزیابی کرد. لازم به ذکر است که میزان تأثیر قدرت سایبری در ارزیابی امنیت و اقتدار کشورها رابطه‌ی مستقیمی با میزان نفوذ دشمنان آن‌ها در فضای سایبری دارد که با توجه به دامنه‌ی وسیع سلطه‌ی دشمنان نظام مقدس جمهوری اسلامی ایران در فضای سایبری، مؤلفه قدرت سایبری، امروزه می‌تواند جزء مهم‌ترین ملاک‌های سنجش امنیت و قدرت کشور باشد. لذا هدف اصلی این تحقیق بررسی تهدیدات در فضای سایبری و تأثیرات آن بر امنیت و اقتدار کشور است.

در این تحقیق پس از بررسی تهدیدات در فضای سایبری و تأثیرات آن بر امنیت و اقتدار کشور سعی شده است بابیان اصولی امنیتی در استفاده از فضای سایبری، حفاظت دقیق‌تری را پیشنهاد داد.

لازم به ذکر است در حین اینکه باید فضای سایبری به‌عنوان تهدیدی جدی برای امنیت و اقتدار کشور تلقی شود، در صورت اتخاذ راهبرد مناسب جهت کنترل تهدیدات و ایجاد هوشمندانه‌ی فرصت‌ها، همین فضای سایبری شامل مجموعه‌ی وسیعی از ابزارهایی است که می‌توانند پایه‌های امنیت و اقتدار کشور را بیش‌ازپیش مستحکم‌تر کرده و نقش مؤثرتری را در این مهم ایفا کند. ازاین‌رو استفاده از فضای سایبری و در ذیل آن شبکه‌های اجتماعی ابتدا تهدیدی جدی و سپس فرصتی عالی به شمار می‌روند.

واژگان کلیدی
تهدیدات فضای سایبری، امنیت کشور، اقتدار کشور، نقش فضای سایبری در امنیت و اقتدار

---

۱. مدرس دانشگاه افسری و تربیت پاسداری امام حسین(ع) ,jalali Ali@Gmail.com
۲. مدرس دانشگاه افسری و تربیت پاسداری امام حسین(ع) saadatmand.a@ihuo.ac.ir

مقدمه

پدیده فناوری اطلاعات و ارتباطات و ابزارهای مربوط به آن، بی‌شک تحولات گسترده‌ای را در تمامی عرصه‌های اجتماعی، اقتصادی، امنیتی و ... را به دنبال داشته و تأثیر آن بر جوامع بشری به‌گونه‌ای بوده است که جهان امروز را به جامعه‌ای اطلاعاتی تبدیل کرده است. جامعه‌ای که در آن دانایی و میزان دسترسی و استفاده مفید از دانش، نقشی محوری و تعیین‌کننده‌ای دارد. در چنین جامعه‌ای دسترسی به رایانه و شبکه جهانی اینترنت به‌عنوان دو نمونه از شاخص‌های مهم توسعه فناوری محسوب می‌شوند.

آمار سامانه‌ی مدیریت ضریب نفوذ اینترنت کشور بیان‌کننده‌ی ضریب نفوذ ۸۲/۱۲ درصدی اینترنت در ایران است که این عدد خود نشان‌دهنده میزان اهمیت موضوع فضای مجازی و نرخ بالای نفوذ آن در جامعه ایران است.

روش تحقیق

با روند رو به رشد اینترنت و در ذیل آن ایجاد گروه‌های سیاسی مجازی و انجمن‌هایی که منافع مشترکی را پیگیری می‌کنند، انتقال مستقیم اندیشه‌ها و دیدگاه‌های جریان‌ها معاند به داخل و ایجاد گروه‌های فشار و ذی‌نفوذ مجازی رسماً دارای برخی وجوه بالقوه‌ی پرمخاطره برای نظام سیاسی جمهوری اسلامی ایران و دست‌آورده‌ای انقلاب بوده که با عنایت به مأموریت سپاه مبنی بر کشف، شناسایی، بررسی، پیگیری، مقابله و خنثی‌سازی طرح‌ها، برنامه‌ها و فعالیت‌هایی که منجر به براندازی، جاسوسی، خرابکاری و اختلال در اداره کشور است این موضوعات در اینجا اهمیتی ویژه‌ای می‌یابند.

لذا طبق نص صریح قانون اساسی دفاع از نظام اسلامی و دستاوردهای آن در حوزه فضای سایبری بخشی از مأموریت‌های سپاه پاسداران انقلاب اسلامی ایران را شامل می‌شود.

در تحقیق حاضر به بررسی قابلیت‌های فناوری اطلاعات و ارتباطات و آسیب‌پذیری‌ها و تهدیدهای متوجه این فن‌آوری پرداخته و ضمن شناخت تهدیدات و آسیب‌پذیری‌ها در حوزه سایبری؛ به بیان نقش اطلاعات در شناخت فضای سایبری و همچنین راهکارهای رفع تهدیدات و آسیب‌پذیری این فضا پرداخته می‌شود.

ضرورت توجه اطلاعات در فضای سایبری

هدف از جنگ سایبری، تخریب سیستم‌های اطلاعاتی و ارتباطاتی هست؛ تلاش این جنگ در جهت شناسایی مسائلی است که دشمن به‌شدت از آن‌ها محافظت می‌کند؛ این جنگ حرکتی در جهت تغییر «توازن اطلاعات و دانش» به نفع یک‌طرف است. به‌خصوص اگر توازن نیروها برقرار نباشد. درواقع، به کمک دانش و سرمایه، نیروی کاری کمتری هزینه خواهد گردید. این جنگ از فناوری‌های گوناگونی بهره می‌برد. از موارد برجسته‌ی این نوع فناوری‌ها می‌توان به فرماندهی و کنترل برای رسیدن به هوشمندی، توزیع و پردازش برای رسیدن به ارتباطات تاکتیکی، تثبیت موقعیت و شناخت هویت دوست و دشمن درزمینهٔ مبادلات سیستم‌های جنگی هوشمند اشاره کرد. همچنین این نوع فناوری‌ها می‌توانند باعث اغفال، فریب و ایجاد اختلال در تجهیزات ارتباطاتی و اطلاعاتی دشمن شده و راهی جهت نفوذ به آن پیدا کنند. جنگ سایبری الزامات گسترده‌ای برای دکترین و سازمان‌های نظامی دارد. حرکت به سمت ساختار شبکه‌ای تا حدودی نیازمند فرماندهی و کنترل غیرمتمرکز است.

جنگ سایبری می‌تواند باعث خلق دکترین جدید درزمینه‌ی انواع نیروهای موردنیاز و اینکه چگونه و کجا باید آنان را مستقر کرد تا بتوان به دشمن تاخت باشد. این‌که چه نوع حسگرها، سامانه‌ها، شبکه‌ها و پایگاه داده‌ها، چطور و در چه موقعیتی قرار گیرند، اهمیتی هم‌سطح با نحوه استقرار بمب‌افکن‌ها و عملیات پشتیبانی آن‌ها درگذشته دارد.

جنگ سایبری می‌تواند همان «حمله رعدآسا» قرن بیستم در قرن بیست و یکم (به‌عنوان ابتکاری در جنگ) باشد. پایین‌ترین سطح جنگ سایبری، مبین اهمیت گسترش اطلاعات در جنگ است. فرماندهی و کنترل، ارتباطات و آگاهی می‌تواند در شناسایی، تعیین موقعیت، فهم و اغفال دشمن (قبل از اینکه دشمن این کار را انجام دهد) مثمر ثمر باشد.

شاید صحنه نبرد در عصر فراصنعتی، تغییرات بنیادینی را در اثر انقلاب فناوری اطلاعات به خود ببیند. افزایش وسعت و عمق میدان نبرد و بهبود مستمر دقت و تخریب‌کنندگی تسلیحات متعارف، اهمیت اطلاعات را به‌جایی رسانده است که برتری تنها از این بعد می‌تواند معنا داشته باشد.

درواقع جنگ سایبری نه‌تنها می‌تواند همان ویرانگری را داشته باشد که جنگ‌های نظامی دارند بلکه عملاً می‌تواند اثر مخرب ویران‌کننده‌تری نیز با خود رقم بزنند.

لذا سپاه پاسداران انقلاب اسلامی نیز در معرض این آسیب‌ها بوده و طبیعتاً بخش‌های مختلف آن به‌ویژه در تمامی رده‌های فرماندهی و کنترل در معرض آفند سایبری است که علاوه بر مأموریت صیانت از دستاوردهای نظام، حفاظت از ساختار و بدنه سپاه به‌عنوان یک واحد منسجم نظامی قطعاً نیازمند توجه ویژه به ابعاد حفاظت در فضای نبرد تحت سایبری است.

مبانی نظری تحقیق

در سال ۱۹۸۶ بر اساس مطالعه‌ای که توسط کارگزاران و مدیران اجرای سیستم‌های اطلاعات[1] انجام شد، بر اهمیت و نقش حیاتی مدیریت سیستم‌های اطلاعات تأکید گردید و ارتقا و بهبود برنامه‌ریزی استراتژیک در درجه اول اهمیت قرارداده شد. یک برنامه‌ریزی مؤثر نیازمند نظم و توان پیش‌بینی مشکلات (تهدیدها) و نیز دارا بودن قابلیت توسعه استراتژی‌ها و سیاست‌هایی بر اساس فنّاوری‌های اطلاعات است که به‌سرعت در حال تغییرند. برای رسیدن به این منظور باید در رابطه با تشخیص فرصت‌های استراتژیک فنّاوری اطلاعات و شناسایی تهدیدات اهتمام ویژه‌ای ورزید که در این طرح از روش جمع‌آوری میدانی به شکل Job box و روش کتابخانه‌ای در تعریف فرصت‌ها و تهدیدات استفاده گردیده و سپس با استفاده از کارشناسان خبره و با روش FGD به تولید یک نتیجه‌گیری عمومی جهت رسیدن به اهداف مقاله اقدام گردیده است.

در منظر عمومی بخش اول این بررسی می‌تواند درنهایت به تعاریف فضای مأموریتی اختصاصی واحدهای جنگ اینترنتی، جنگال (جمع‌آوری الکترونیک)، سازمان اطلاعات و قرارگاه‌های اختصاصی و یا مشترک سایبری ختم شود.

اما در بخش دوم تمرکز بر اهداف استراتژیک سپاه پاسداران انقلاب اسلامی در فعالیت‌های تحت پشتیبانی فنّاوری اطلاعات است که می‌توانند برای تحت تأثیر قرار دادن و برخورد با اهداف به کار گرفته شوند. در این فرایند فهرستی از فعالیت‌های ممکن را پدید آورده است که با استفاده از این فهرست می‌توان اهدافی را برای هجوم و یا دفاع توسط سپاه اتخاذ نمود.

1. Information Systems

امنیت و اقتدار کشور

امنیت صرفاً جنبه فیزیکی نداشته بلکه مهم‌تر از امنیت مالی و جانی احساس امنیت است. احساس امنیت همان‌گونه که جزء بدیهی‌ترین نیاز هر انسان تلقی می‌گردد، از اساسی‌ترین احتیاجات هر حکومت نیز محسوب می‌گردد. برای هر ملتی، آرمانی‌ترین حکومت، دولتی است که بتواند بالاترین احساس امنیت را برای شهروندان به ارمغان آورد.

در این تحقیق منظور از امنیت «وجود یک فضای باثبات به‌ویژه در فضای روانی کشور می‌باشد.» که این امنیت خود یکی از اصلی‌ترین مؤلفه‌های اقتدار می‌باشد.

فضای سایبر

واژه سایبر، از لغت یونانی کیبرنتس،[1] به معنی سکان‌دار یا راهنما مشتق شده است. نخستین بار، این اصطلاح «سایبرنتیک»، توسط ریاضیدانی به نام نوربرت وینر،[2] در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین»، در سال ۱۹۴۸ به‌کاربرده شده است. سایبرنتیک علم مطالعه و کنترل مکانیسم‌ها در سامانه‌های انسانی، ماشینی (کامپیوترها) است.

سایبری عبارت است از؛ محیط الکترونیکی واقعی، که در آن ارتباطات انسانی به شیوه سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود به‌طور زنده و مستقیم روی می‌دهد. مثل اینترنت و بلوتوث (جمشید محبی، ۱۳۸۹).

سایبری پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه‌های ترکیبی بسیاری از این کلمه سایبری به وجود آمده است مانند:

فضای سایبر،[3] شهروند سایبر،[4] پول سایبر،[5] فرهنگ سایبر،[6] راهنمایی فضای سایبر،[7] تجارت سایبر،[8] کانال سایبر[1] و ...

---

1. Kybernetes
2. Wienernorbert
3. Cyberspace
4. Cybercitizen
5. Cybercash
6. Cyberculture
7. Cybercoach
8. Cyberbussiness

به‌عبارت‌دیگر، فضای سایبری مجموعه‌ای است سازمان‌یافته از شبکه‌های رایانه‌ای شامل: نیروی انسانی، زیرساخت‌ها، تجهیزات، سخت‌افزار، نرم‌افزار و سامانه‌های ارتباطی، کنترلی و مدیریتی به‌منظور تولید، ذخیره‌سازی، پردازش و انتقال و بهره‌برداری از اطلاعات. به‌عنوان نمونه، یک سیستم برخط (آنلاین) نمونه‌ای از فضای سایبری است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبری نیاز به جابه‌جایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات موشواره (ماوس) صورت می‌گیرد.

امنیت سایبری

امنیت سایبری را به‌عنوان پارامتری ضروری در دنیای سایبری، به‌صورت زیر تعریف می‌کنیم: «ایجاد بستری امن، برای کاربران فضای سایبری که در آن سوءاستفاده از داده‌های سایبری وجود نداشته باشد.»

انتظار چنین چیزی، تقریباً غیرممکن است، ولی با روش‌هایی چون رمزگذاری داده‌ها، جداسازی داده‌ها و تفکیک پایگاه‌های داده می‌توان تا حدود امنیت را در فضای سایبری حاکم کرد[۱]. حریم خصوصی جز ضروری در فضای سایبری است و استراتژی‌های امنیت فضای سایبری باید به روش‌های سازگار باارزش‌های مهم جامعه پیاده‌سازی شوند.

[Simson, Garfinkel, Spafford, Gene, and Schwartz, Alan, "Practical Unix and Internet Security", 3rd Edition, Cambridge, Ma:OReilly and Associates, 2003…]

جنگ سایبری[۲]

ایجاد اختلال در سامانه‌های اطلاعاتی و ارتباطی و زیرساخت‌های حیاتی بر پایه فناوری اطلاعات که دشمن برای افزایش دانش خود به آن‌ها تکیه می‌کند را جنگ سایبری گویند [۳]. هدف اصلی این جنگ، بر هم زدن موازنه اطلاعات و دانش در سطح کشور هدف است. نقطه آغازین در این جنگ، اینترنت بوده و برخی از ویژگی‌هایی که این جنگ دارد، ناشناس بودن مهاجم، بهره‌گیری از نقاط ضعف، دشواری کشف اهداف و نقاط حمله و... است.

1. Cyberchannel
2. Cyber War

ویژگی‌های فضای سایبر

در جنگ سایبری، از شبکه‌های رایانه‌ای و مخابراتی به‌عنوان بستر انجام این اعمال خرابکارانه استفاده می‌شود. به‌طورکلی، حملات فضای سایبری به دودسته تقسیم می‌گردد:

الف) حملات خاموش[1] فضای سایبری؛ دست‌یابی به منابع اطلاعاتی و خدماتی هدف موردنظر به‌صورت مخفی، به‌منظور اقدام به تخریب، تحریف، تغییر، سرقت، جعل، سانسور، شنود و بهره‌برداری از آن‌ها را حمله خاموش می‌گویند.

ب) حملات فعال[2] فضای سایبری؛ ایجاد اختلال در فعالیت‌های عادی سامانه‌های هدف که به هر نحو باعث جلوگیری از کار یک سرویس شده و یا مانع دسترسی به منابع گردد را حمله فعال گویند.

جنگ سایبری یا جنگ اطلاعاتی، باهدف از هم گسیختن سامانه‌های اطلاعاتی و مخابراتی، سامانه‌های کنترل و فرماندهی، ارتباطات، خبرگیری و جاسوسی نیروهای نظامی دشمن و غیرعملیاتی کردن آن‌ها درصحنه نبرد صورت می‌گیرد؛ بنابراین، مسئولیت سازمان‌های حفاظتی و اطلاعاتی در شناخت ابعاد مختلف فضای مجازی یا سایبری و جنگ ناشی از آن بسیار سنگین و حساس خواهد بود.

فضای سایبری و جنگ‌های سایبری دارای ویژگی‌هایی هستند که این ویژگی‌ها باعث سهولت در دسترسی، بهره‌برداری و همچنین گسترش آن‌ها شده است و هزینه‌ها را نسبت به جنگ‌های نظامی برای حمله‌کنندگان کاهش داده و برعکس خسارات و آسیب‌ها را برای کشورها و اهداف مورد هجوم واقع‌شده‌ها افزایش داده است. بدین‌جهت در این قسمت برخی ویژگی‌های فضای سایبری به‌اختصار بیان ویژگی‌های جنگ سایبری تشریح می‌گردد؛

ویژگی‌های جنگ سایبری

۱. جهانی و فرامرزی بودن (فاقد مرز جغرافیایی است)

۲. محدوده‌ی عملیاتی

۳. محدوده‌ی جغرافیایی

1. Passive Attack
2. Active Attack

۴. مشخصات عملیات سایبری (شباهت‌ها به دیگر جنگ‌ها)

- ۱ـ۴. انگیزه
- ۲ـ۴. هدف
- ۳ـ۴. جمع‌آوری اطلاعات
- ۴ـ۴. نقاط ضعف
- ۵ـ۴. نفوذ

تهدیدات در فضای مجازی

امروزه برای تضعیف یک کشور و یا حکومت در دنیا لزومی ندارد که به‌طور حتمی اماکن و تأسیسات حساس و مهم آن کشور را بمباران کنند، بلکه یک مودم و یک رایانه کافی است. کریستین‌هاربولوت[1] از دانشکده جنگ اقتصادی آمریکا می‌گوید: سلاح نباید به‌طور حتمی زهر یا تپانچه باشد، بلکه خراب‌کاری در اطلاعات نیز می‌تواند به‌عنوان یک سلاح مخرب به کار گرفته شود. (ویلیام سی. بونی، جرالد آل. کواسیچ: ۱۱)

با گسترش روزافزون استفاده از رایانه در دنیا، تشکیل و گسترش فضای مجازی و غیر فیزیکی به وقوع پیوسته است، ازآنجاکه استفاده از رایانه و فضای مجازی برای اکثر افراد، از نهادهای غیردولتی و دولتی، نیروهای مسلح، وزارت خانه‌ها، سازمان‌ها، ناوبری، حمل‌ونقل، تجارت گرفته تا فعالیت‌های پستی در یک روستا، امری اجتناب‌ناپذیر است، اهمیت توجه به استفاده همه‌جانبه از رایانه‌ها و فضای سایبری به‌اندازه کره زمین و فضای اطراف آن گستره دارد.

وجود و استفاده گسترده از اصطلاحاتی نظیر حمله سایبری، سرباز سایبری، تروریسم سایبری، سلاح سایبری، تهدید سایبری، جنایت سایبری، شهر سایبری و ... بیان‌گر اهمیت این موضوع در جهان و آینده آن است.

شایان‌ذکر است که کارشناسان مسائل امنیتی و اطلاعاتی به‌ویژه آمریکایی‌ها، مهم‌ترین وجدی‌ترین آسیب‌پذیری آمریکا را فضای سایبری می‌دانند.

در ایران نیز اگرچه گستره‌ی استفاده از فضای مجازی به‌اندازه غرب و آمریکا نیست،

1. Christian Harbulot

لیکن آسیب‌پذیری‌های جدی در این حوزه وجود دارد و در سال‌های اخیر به‌ویژه در حوزه جنگ روانی، حوزه ارتباطات، آموزش و هدایت اپوزیسیون داخلی، سرقت و تخریب اطلاعات که بستر آن فضای سایبری بوده، آسیب‌پذیری‌ها به‌طور کامل مشهود خواهد شد.

در وضعیت فعلی کشور متأسفانه به مباحث امنیتی فضای مجازی یا سایبری نیز توجه جدی نمی‌شود و جا دارد بیش‌ازپیش امنیت فضای مجازی موردتوجه قرار گیرد.

انجمن شراکتی نظام‌های الکترونیکی نوت بوک با انتشار گزارشی با عنوان «تایتانیک ـ ۲۰۲۰» نتیجه‌گیری می‌کند که دنیا به‌زودی میلیاردها دلار به خاطر سرقت اطلاعات حساس خسارت خواهد دید، زیرا نرم‌افزارهای مناسب برای جلوگیری از این سرقت ایجاد نشده است. (ویلیام سی. بونی، جرالدال کواسیچ: ۱۲)

اگر یک نوجوان می‌تواند به‌صورت غیرمجاز وارد شبکه‌های رایانه‌ای شود، به‌طور مطمئن عوامل جاسوسی و جاسوسی‌های فنی نیز می‌توانند خیلی راحت‌تر این کار را انجام دهند.

تا اواخر دهه ۱۹۸۰ یک‌راه ساده برای دسترسی به اطلاعات استفاده از یک مودم برای وارد شدن به شبکه‌های رایانه‌ای بود. استفاده‌کننده ممکن بود که رایانه خود را خاموش کند اما شخص غیرمجاز می‌توانست در همان وضعیت وارد شبکه شود و از تمام اطلاعاتی بهره‌مند شود که استفاده‌کننده مجاز به آن دسترسی دارد. امروزه یک ابزار قوی برای جمع‌آوری اطلاعات، ورود از طریق میکروفن و دوربین‌های اینترنتی است. بیل لیونز[1] درزمینهٔ حافظت اینترنتی می‌گوید: «نظامیان آمریکا این روش را آزمایش کرده‌اند و اگر آن‌ها توانسته باشند از این طریق به اطلاعات دسترسی پیدا کنند، مطمئن باشید که افراد غیرمجاز نیز می‌توانند با همین روش وارد شبکه‌های رایانه‌ای شوند. وحشتناک‌تر از همه این است که ابزارهایی روی اینترنت است که می‌تواند میکروفن را روشن کند و صداها را ضبط و به شخص دیگری منتقل کند بدون آن‌که استفاده‌کننده رایانه متوجه شود.» (همان صفحه ۱۵-۱۴)

در فضای سایبری و با حملات سایبری می‌توان برج‌های مراقبت فرودگاه‌ها، اتاق کنترل قطارها، چراغ‌های راهنمایی در خیابان‌ها، اتاق کنترل دریچه‌های سدها، نیروگاه‌ها، بانک‌ها و تجارت الکترونیک، بورس، پادگان‌های نظامی، کارخانه‌های جنگ‌افزارسازی، وزارت خانه‌ها،

1. Bill Lyons

شبکه‌های ارتباطی، سوخت‌رسانی، ماهواره‌ها، سامانه‌های موشکی و ... را مورد هجوم قرارداد. در چنین جهانی و با چنین آسیب‌هایی چه می‌توان کرد؟

قرن ۲۱ که خیلی از بازیگران عمده انتظار دارند که «عصر اطلاعات» باشد ممکن است «عصر جاسوسی» و یا عصر «جنگ جهانی سایبری» باشد.

مصادیق و نمونه‌های حملات و جنگ‌های سایبری

به گزارش منابع غربی، اولین جنگ سایبری در کوزوو، رخداده است، اما چنین نیست، این ادعا به‌نوعی سبب پوشش جنگ‌های متعدد سایبری می‌گردد که همگی در دوران جنگ سرد (۱۹۱۷-۱۹۹۱) در ۲۴ شکل و دوره متفاوت به وقوع پیوسته‌اند. برخی عناوین جنگ‌ها و حملات معروف و ثبت‌شده سایبری عبارت‌اند از؛

کره شمالی و آمریکا ـ از دهه ۸۰ ـ کره شمالی اقدام به تأسیس مدرسه هک با بیش از ۱۰۰ سرباز آموزش‌دیده می‌نمایند. البته این عمل در حقیقت عکس‌العملی در برابر توان مضاعف دشمن است. جنگ‌های این دهه را می‌توان پیامدهای مشخصی از جنگ سرد دانست؛ بنابراین، انگیزه‌ها به‌طور کامل مشخص هستند. (کاوه سید مفیدی صفحه ۸)

بین آوریل و می سال ۱۹۹۱ـ پنج هکر هلندی به سامانه‌های رایانه‌ای ۳۴ سایت نظامی آمریکا در اینترنت ازجمله سایت‌هایی که به‌طور مستقیم عملیات سپر توفان صحرا را پشتیبانی می‌کردند نفوذ کردند. آن‌ها در پست‌های الکترونیکی و فایل‌ها به جستجو پرداختند و به دنبال کلمات کلیدی همچون هسته‌ای، سلاح، موشک، سپر صحرا و توفان صحرا بودند. آن‌ها اطلاعاتی مربوط به موقعیت دقیق نیروهای آمریکایی، نوع سلاح‌ها، قابلیت‌های موشک‌های پاتریوت و حرکت ناوهای جنگی آمریکا در منطقه خلیج‌فارس را به دست آوردند. [دی.ای دنینگ، جنگ اطلاعات و امنیت، صفحه ۲]

سال ۱۹۹۴ ـ حمله به مراکز هوایی و تحقیقاتی Room در نیویورک و هم‌زمان به انستیتو تحقیقات اتمی کره جنوبی و درنهایت مرکز علمی در لاتویا (از کشورهای تازه استقلال‌یافته شوروی سابق) [همان]

سال ۱۹۹۵ ـ بانک معروف آمریکایی CitiBank و گروه هکرهای روسی و از دست دادن ۴۰۰ هزار دلار. درنهایت حمله هکرهای روسی شناسایی‌شده و بخشی از زیان‌ها جبران شد [همان].

ماه می سال ۱۹۹۹ ـ براساس دستور بیل کلینتون، رئیس‌جمهور وقت ایالات‌متحده آمریکا، CIA طرح حمله به سامانه‌های رایانه‌ای یوگسلاوی را پی‌ریزی می‌نماید. این همان جنگی است که به سبب فاش شدن اسرار آن، مقامات آمریکایی راه گریزی از آن نمی‌بینند و آن را به‌طور رسمی تائید می‌نمایند. از پیامدهای این جنگ می‌توان به موارد ذیل اشاره نمود:

- نفوذ به‌حساب‌های بانکی
- قطع نمودن خطوط تلفن
- تهدید مراکز سوخت‌رسانی و غذا

سپتامبر سال ۱۹۹۹ـ جنگ ۷۸ روزه. وزارت دفاع آمریکا، طرح حمله به شبکه‌های کامپیوتری «سرب» را با جدیت ادامه می‌دهد.

اهداف: تهدید تسلیحات نظامی و خدمات اجتماعی

اوایل اوت سال ۲۰۰۰ـ هنگ‌کنگ و استفاده از جنگ سایبری علیه چین

استفاده از ویروس‌ها در هدف قرار دادن مراکز انرژی، نظامی و بانک‌ها

اسرائیل و فلسطین، جنگ اعراب و اسرائیل و درنهایت کشیده شدن جنگ به آمریکا [همان]

تهدید سایت‌های اینترنتی طرفین

حملات متناوب داس[1]

حضور اعراب در برابر اسرائیل در این جنگ‌ها محسوس است؛ بنابراین، نمی‌توان فقط فلسطین را مدنظر داشت.

تکرار زمانی: اوایل نوامبر سال ۲۰۰۰ و اواسط آوریل سال ۲۰۰۲

مارس و آوریل سال ۲۰۰۱- آمریکا و چین بر سر موضوع تصادف هواپیمای جاسوسی آمریکا با جت چینی [سید مفیدی، ۹]

سایت دولتی چین[2]، اولین قربانی

این جنگ تا حدودی به اروپا کشیده شد.

درصد تخریب در چین ۱۰ برابر آمریکا بود.

1. DOS Atack
2. www.travelsichuan.gov.cn

نزدیک به ۱۰۰ حمله سایبری بین آمریکا و چین درگرفته است که این مشهورترین آن‌هاست.

آوریل سال ۲۰۰۱- آمریکا و روسیه [همان: ۱۰]

ـ استفاده از هکرهای روسی برای نفوذ به شبکه خدمات امنیتی کشور روسیه

یازده سپتامبر ۲۰۰۱- یک شروع مجدد و هزاران علامت سؤال

طبق شواهد، حملات تروریستی این ماه در نیویورک واشنگتن، حداقل دارای پشتوانه سایبری بوده است.

ـ آمریکا مسئولیت را به‌طور مشخص به گروه القاعده نسبت می‌دهد.

ـ شواهد نشان‌گر طرح‌ریزی بسیار دقیق و اجرای عملیات طی حدود یک سال و نیم است.

۱۲. ماه می سال ۲۰۰۳- آمریکا و عراق بر سر موضوع تجاوز به عراق [همان: ۱۰]

ـ این بیشتر یک جنگ سایبری تبلیغاتی بود تا نظامی

۱۳. اوایل سپتامبر سال ۲۰۰۳- چین علیه تایوان؛ چین مبادرت به حمله سایبری به دولت تایوان می‌نماید. [همان: ۱۱]

ـ این حمله از طریق انتشار اسب‌های تروآ[1] محقق گردید.

۱۴. اکتبر سال ۲۰۰۳- حمله به یکی از بزرگ‌ترین فرودگاه‌های ایالات‌متحده در بوستون/ تگزاس [همان: ۱۱]

۱۵. مارس سال ۲۰۰۴- آخرین جنگ دونفره- Netsky و My Doom- آیا به‌طور حقیقی دو نفر در این جنگ آسیب می‌بینند؟ [همان: ۱۱]

۱۶. یک جوان ۲۳ ساله آرژانتینی داوطلبانه به آمریکا رفت تا به اتهام هک کردن سیستم رایانه‌ای دانشگاه‌ها و سیستم رایانه‌های نظامی آمریکا محاکمه شود. گفته می‌شود که وی به اطلاعات حساس اما غیر محرمانه‌ای درزمینه‌ی ماهواره، تشعشع و مهندسی انرژی دست‌یافته بود. وی به سه سال حبس تعلیقی و پرداخت پنج هزار دلار جریمه نقدی محکوم شد. [همان: ۱۱]

سالانه ۲۵۰ هزار حمله سایبری به مراکز نظامی آمریکا صورت می‌گیرد که فقط اندکی از آن‌ها تأثیرگذار می‌شوند. [همان: ۱۱]

سالانه حدود نیم میلیارد دلار به آمریکا خسارت وارد می‌شود.

1. Trojan

کارشناسان معتقد هستند در بین کشورهای پیشرفته، ژاپن به علت نداشتن سیاست‌های امنیت اطلاعاتی، یکی از ضعیف‌ترین اهداف سایبری محسوب می‌گردد [سید مفیدیِ، ۱۲-۸].

حمله هکری به خبرگزاری‌ها و سایت‌های رسمی در فتنه ۸۸ ازجمله سایت مقام معظم رهبری، سایت خبرگزاری فارس، سایت خبرگزاری ایسنا، سایت مجلس شورای اسلامی، سایت دانشگاه پیام نور و سایت گرداب (محبی، ۱۳۸۹)

بیشترین فعالیت دشمن در فتنه ۸۸ در بستر فضای سایبری شامل: آموزش اغتشاش‌گران، ایجاد ارتباط امن در اینترنت برای مخالفان و آشوبگران، ایجاد فیلترشکن‌ها، عملیات روانی با راه‌اندازی سایت‌های مختلف و متعدد در حجم وسیع علیه نظام و سپاه، اطلاع‌رسانی به مخالفان و اغتشاش‌گران (محل‌های تجمع مسیرهای حرکت و ...)

آخرین نمونه حمله سایبری در ایران مربوط به آلوده نمودن سامانه‌های رایانه‌ای نیروگاه هسته‌ای بوشهر با استفاده از کرم استاکس نت در اواخر سال ۲۰۱۰(پاییز ۱۳۸۹) است که هدف آن اختلال در فعالیت‌های هسته‌ای ایران بوده است. به‌گونه‌ای که این ویروس در نرم‌افزاری مورداستفاده فعال می‌شود که به‌طورقطع آخرین حمله سایبری در ج.ا.ا نخواهد بود. هم‌اکنون که در حال مطالعه این مطالب هستید، در گوشه‌ای از جهان یک حمله سایبری در حال برنامه‌ریزی و حمله سایبری دیگری در حال اجرا است.

بخشی از پشت پرده‌های فضای مجازی بخصوص شبکه‌های اجتماعی

استخدام روزنامه‌نگار و مفسر اینترنتی توسط اسرائیل (خبرگزاری فارس ۱۵ فرودین ۱۳۹۰)

استخدام بیش از ۲۵۰۰ نفر روزنامه‌نگار به‌منظور رصد ۲۴ ساعته پایگاه‌های اینترنتی بخصوص فیس‌بوک[1] و نگارش تفسیرهای جانب‌دارانه درباره اسرائیل

«رابرت گیتس» وزیر دفاع وقت آمریکا در ژوئن ۲۰۰۹ اعلام کرد، فنّاوری‌های رسانه‌های اجتماعی همچون توییتر[2] که نقشی حیاتی در مستندسازی و هماهنگی اعتراضات در ایران به‌ویژه تهران داشتند، یک دارایی استراتژیک عظیم برای آمریکا محسوب می‌شوند.

برنامه ۲۸ میلیون دلاری وزارت خارجه آمریکا در امتداد بودجه ۵۰ میلیون دلاری

1. Facebook
2. Twitter

عبور از فیلترینگ و برنامه دیگر ساخت یک نرم‌افزار و تعبیه یک «دکمه وحشت» برای تلفن‌های موبایل که فعالان به اصلاح سیاسی می‌توانند از آن برای ژاک کردن آدرس‌ها در صورت بازداشت استفاده کنند (خبرگزاری فارس).

یکی از سیاست‌های فضای مجازی مرزهای شیشه‌ای است. به‌ویژه در شبکه‌های اجتماعی؛ کاربر در شبکه‌های اجتماعی به بهانه داشتن ارتباطات گسترده، مدام در حال ارائه اطلاعات شخصی خود به شکل عمومی است! درواقع مدام در معرض این شعار تبلیغاتی قرار دارد که «اگر می‌خواهید همه‌جا باشید، بگذارید همه به اطلاعات شما دسترسی داشته باشند» به‌کارگیری و تخلیه اطلاعاتی مخاطب بدون اینکه وی کوچک‌ترین آگاهی از این امر داشته باشد.

کرم‌ها و تروجان‌ها در شبکه‌های اجتماعی (در قالب فیلم، لینک و...)

سرقت هویت (نام کاربری و پسورد).

مدتی پیش ایمیلی برای کاربران فیس‌بوک ارسال شد که از آن‌ها می‌خواست در اتصالی (لینکی) که در ظاهر متعلق به فیس‌بوک بود، ثبت‌نام (لاگین) کنند که این موضوع خود یک هک اطلاعات بود.

نشت داده‌ها

مهم‌ترین کار در شبکه‌های اجتماعی، «به اشتراک گذاردن» داده‌های مختلف با دیگران است. متأسفانه بسیاری از کاربران، اطلاعات بسیار زیادی را راجع به سازمانی که به آن متعلق هستند، پروژه‌ها، محصولات، مسائل مالی، تغییرات سازمانی، رسوایی‌ها و سایر مسائل حساس به اشتراک می‌گذارند.

تأثیر تهدیدات فضای مجازی در جوامع

۱- کمرنگ شدن قوانین سنتی:

۲- شکل‌گیری اجتماع مجازی:

۳- تغییر ذائقه ارتباطی عموم (تضعیف ارتباطات واقعی)

۴- دریافت‌های جایگزین:

۵- جهت‌دهی و هدایت افکار مردم[1]

۶- شکل‌دهی به اعتراضات جمعی و شبکه‌سازی، ایجاد و کنترل اجتماعات، تحولات و بحران‌ها در اجتماع (نقش فیس‌بوک و توییتر) (همان).

۷- تأثیر بر افکار عمومی و بسیج:

۸- جایگزینی ملاقات حضوری با مجازی

برخی از اقدامات عملیات روانی دشمن پس‌ازآنتخابات دهم ریاست‌جمهوری ایران در فضای مجازی

پس‌ازآنتخابات دهم ریاست جمهوری ایران رسانه‌های خارجی به‌ویژه رسانه‌های انگلستان (نظیر تلویزیون فارسی بی‌بی‌سی، رادیو بی‌بی‌سی و سرویس جهانی بی‌بی‌سی) و رسانه‌های آمریکا (تلویزیون صدای آمریکا، سایت اینترنتی آن، رادیو فردا و شبکه CNN) با تدابیر از پیش اندیشیده شده، عملیات روانی گسترده‌ای را علیه جمهوری اسلامی طراحی و اجرا نموده‌اند.

آن رسانه‌ها با استفاده از اصولی نظیر تکرار، ادعا، سرایت، حیثیت منبع، القاء و بهره‌گیری از فنونی نظیر تهییج، دروغ بزرگ، شایعه، نام‌گذاری، تبخیر، تشابه و تداعی، بزرگ‌نمایی، تحقیر، تخدیر، تقطیع و غیره می‌کوشیدند (و همچنان می‌کوشند) تا به بزرگ‌نمایی اعتراضات داخل و خارج ایران بپردازند.

آن رسانه‌ها با نمایش مکرر چهره فرمانده ناجا (سردار احمدی مقدم) و جانشین ناجا (سردار رادان) و هم‌زمان ساختن نمایش این چهره‌ها با ضرب و شتم چند نفر از معترضان توسط افراد ملبس به لباس پلیس، چنین به مخاطبان القاء می‌کردند که عامل اصلی خشونت‌های رخداده در روزهای بعدازآنتخابات، این دو نفر هستند. آن رسانه‌ها حتی پا را از آن فراتر گذاشته و به این دو نفر نصیحت می‌کردند که «تا دیر نشده دست از اعمال خشونت‌آمیز بردارید و به مردم بپیوندید.»

برخی رسانه‌ها (به‌ویژه بی‌بی‌سی و صدای آمریکا) در روزهای پس‌ازآنتخابات از ابتکارات ویژه‌ای نیز استفاده نمودند. زمانی که خبرنگاران و گزارشگران آن‌ها از ادامه

1. www.isfictnews.ir

فعالیت در ایران بازماندند، بلافاصله از خبرنگاران، عکاسان، گزارشگران و فیلم‌برداران «غیرحرفه‌ای» استفاده کردند. این افراد غیرحرفه‌ای به‌سرعت اخبار و گزارش‌های مربوط به کنش‌های اعتراض‌آمیز داخل ایران را به آن شبکه‌ها منتقل می‌نمودند و آن رسانه‌ها نیز بلافاصله مبادرت به پخش آن می‌کردند. این گزارشگران غیرحرفه‌ای که در سراسر ایران سازمان‌دهی شده‌اند، در طول ۲ ماه پس‌ازآنتخابات صدها گزارش تصویری، تلفنی و نوشتاری برای شبکه‌های خارجی تهیه و ارسال نمودند.

برخی از اقدامات سایبری دشمن در ایام فتنه

جستجوگر گوگل بلافاصله پس‌ازآنتخابات، نرم‌افزار مترجم خود را فعال نمود تا امکان ترجمه پیام‌های فارسی به زبان‌های دیگر و یا از زبان‌های دیگر به فارسی را فراهم سازد، اقدامی که قرار بود چند ماه بعد صورت گیرد.

سایت‌های توییتر و فیس‌بوک امکان بهره‌گیری فزون‌تر را برای کاربران ایرانی فراهم ساختند. به‌گونه‌ای که این دو سایت به رسانه‌ای ویژه برای معترضان تبدیل شدند.

شبکه تلویزیونی بی‌بی‌سی از روز انتخابات تا چند روز پس‌ازآن برنامه‌های خود را از ۷ ساعت به ۲۴ ساعت افزایش داد.

روسای چند کشور اروپایی و آمریکا به‌صورت مستقیم علیه نظام موضع‌گیری کردند و شایعه تقلب در انتخابات را به‌عنوان واقعیت به شهروندان خود معرفی نمودند.

بلافاصله پس از قتل کسانی همچون ندا آقا سلطان، صحنه قتل در هزاران سایت و رسانه خارجی انعکاس یافت.

ارائه خدمات VPN مجانی جهت مخفی ماندن ارتباطات و همچنین گذر از فیلتر قانونی

راه‌اندازی SMS Center و ارسال پیامک

راه‌اندازی دریافت تصاویر تلویزیونی توسط پهنای اینترنتی کم

ارتباط و هدایت عوامل داخلی از طریق (سایت، ایمیل، گروه‌های خبری)

ایجاد سایت‌های متعدد خبری با امنیت بالا

امن سازی میل سرورهای اینترنتی با استفاده از پروتکل HTTPS

آموزش اینترنتی عوامل فتنه (امنیت فن‌آوری اطلاعات و ارتباطات)

آسیب‌های کارکنان سازمان‌های نظامی و اطلاعاتی در فضای سایبری

باگذشت زمان و با توجه به آن‌که تعداد افرادی که از طریق اینترنت به هم متصل شده بیشتر شده و در ذیل آن تقاضا برای دسترسی به اطلاعات از راه دور، حجم اطلاعات بر روی شبکه‌ها و اینترنت زیادتر و امکان ارتباط بین افراد و سازمان‌ها آسان‌تر می‌شود، بخش وسیعی از خانواده‌ی بزرگ نیروهای مسلح نیز به‌عنوان کاربران عمومی و یا اختصاصی اینترنت در معرض خطر قرار می‌گیرند. همین موضوع باعث می‌شود که رخنه به اطلاعات رده‌ها آسان‌تر از عبور از حفاظت فیزیکی آن‌ها شود. این اطلاعات ممکن است شامل اطلاعات طبقه‌بندی‌شده ازنظر رده‌های مسئولیتی و یگان‌های عملیاتی باشد. ردوبدل اطلاعات در اینترنت بین سازمان‌ها و یا کاربران آن و حجم اطلاعات موجود در شبکه‌ها سبب گردیده است که مانند فضای واقعی، حفاظت بر ارکان و فعالیتی فضای سایبری شامل افراد (کاربران)، تجهیزات و نقل و انتقالات (اطلاعات) مترتب باشد.

آسیب‌هایی که تاکنون بیان گردید، به‌صورت عام متوجه تمام مردم، نیروهای نظامی و سازمان‌های غیردولتی و دولتی ازجمله بخش‌های نظامی و امنیتی هست؛ لیکن، برخی آسیب‌های خاص وجود دارد که هدف آن‌ها بیشتر بخش‌های نظامی، امنیتی و اطلاعاتی است که مهم‌ترین آن‌ها عبارت‌اند از:

۱. ردیابی و مکان‌یابی با استفاده از فضای سایبری
۲. استخدام و جذب منابع
۳. تخلیه اطلاعات با ابزارها و روش‌های فنی

توصیه‌ها و راه‌کارهای مقابله با حملات سایبری

الف) اشراف اطلاعاتی در فضای سایبری
ب) حمله و اقدامات آفندی در فضای سایبری
ج) دفاع و اقدامات پدافندی در فضای سایبری

مدل حفاظتی و امنیتی مبتنی بر اصول و تدابیر حفاظتی

۱. اصلاح و تغییر ساختار دستگاه‌های حفاظتی و اطلاعاتی
۲. ایجاد مدیریت امنیت اطلاعات در فضای سایبری

۳. شناسایی نیازمندی‌های امنیتی
۴. ایجاد سیستم کنترلی (اتخاذ و اجرای کنترل‌های مناسب)
۵. رعایت اصل محرمانگی (عدم افشاء)
۶. طبقه‌بندی حفاظتی
۷. حیطه‌بندی
۸. کنترل دسترسی (محدود نمودن دخل و تصرف کارکنان و کاربران در اطلاعات)
۹. سایر تدابیر و اصول حفاظتی برای ایجاد امنیت اطلاعات در فضای سایبری

نتیجه‌گیری و پیشنهادها

سامانه‌های اطلاعاتی دشمن، به‌طور مدام و گسترده فعالیت می‌کنند تا نیازمندی‌های اطلاعاتی خود را به دست آورند. دشمن با تمام توان و با به‌کارگیری مدرن‌ترین سلاح‌ها و ابزارهای اطلاعاتی در گردآوری اطلاعات تلاش پیگیر دارد و با شیوه‌های گوناگون درصدد کشف تازه‌ترین اخبار طبقه‌بندی و غیر طبقه‌بندی است.

ازآنجاکه پس از پیروزی شکوهمند انقلاب اسلامی، جنگ اطلاعاتی و امنیتی تمام‌عیاری علیه جمهوری اسلامی ایران در حوزه‌ی فضای سایبری شکل گرفت، لازم است تا با تمرکز بیشتری پیرامون پژوهش در این دنیای پیچیده به دنبال آن باشیم تا در مقابل ظهور جنگ‌افزارهای فناورانانه دشمن، ابزارهایی به‌مراتب قوی‌تر را وارد میدان این نبرد کنیم.

در پایان باید متذکر شد که با پیشرفت روزافزون فناوری‌هایی که مسلماً دشمنان قسم‌خورده‌ی نظام مقدس جمهوری اسلامی ایران بیش از ما به آن توجه دارند، عرصه‌ی دفاع سایبری پیچیده‌تر و با گذر زمان و عدم توجه کافی سخت‌تر نیز خواهد شد. قبل از آنکه دشمن جاهل ما فکر غلبه بر ما در میدان سایبری را به ذهن خود راه دهد، باید پایه‌های پژوهش خود درزمینهٔ‌های جدید فناوری اطلاعات را مستحکم‌تر ساخته تا سپاه اسلام همچون تمام جبهه‌ها، در این جبهه‌ی نوظهور نیز پیروزی نهایی خود را جشن بگیرد.

ازاین‌رو، نباید هیچ‌گاه از دشمن غافل شد و یا او را کوچک و ناچیز

شـمـرد. در جریان جهانی که امروزه به‌جایی رسیده است که میدان‌های سنتی جنـگ یعنـی زمین، هوا، دریا و فضا جای خود را به میدان بسیار پیچیده و پرتلاطم جدیدی یعنـی میـدان سایبری داده‌اند، نمی‌توان ساده نشست و دست روی دست گذاشت. امروزه مهم‌تـرین مؤلفـه امنیت و اقتدار هر کشوری مؤلفه سایبری آن است. چراکـه میـدان رزم در معـادلات امـروزی جهان تغییر کرده و در حمله و دفاع، تبحر سایبری حرفی اساسی خواهد داشت.

باید تلاش مجدانه‌ای کرد که ابتدا موضوع سایبری و امنیت آن را به موضـوعی حیـاتی در ذهن مسئولین کشور و همچنین سپاه تبدیل ساخت. پس‌ازآن باید طرح‌ریزی پـروژه‌ای را رقم زد که جایگاه درسـت و فنـی قـدرت سـایبری در امنیـت و اقتـدار کشـور را علمـی محاسبه نماید. در انتها پس از احصاء نیازمندی‌های تخصصی باید به هدف ایجـاد امنیـت و اقتدار پایدار کشور با تکیه‌بر قدرت سایبری ایران اسلامی پروژه‌ای ملـی تـدوین و آن را در میان تمام دستگاه‌های دولتی، حاکمیتی و حتی اقشار و آحاد مردم فرهنگ نمود.

منابع و مآخذ

ـ حسن بیگی، ابراهیم، «حقوق و امنیت در فضای سایبر»، موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران، ۱۳۸۴.

ـ حسینی‌نیا، شاهپور، (۱۳۸۵)، اینترنت و امنیت اطلاعات، تهران، دانشگاه امام حسین علیه‌السلام.

ـ حسینی، سیدحسین (۱۳۷۱)، تبلیغات و جنگ روانی، تهران، دانشگاه امام حسین علیه‌السلام، پژوهشکده علوم دفاعی.

ـ خواجه نصیری تابان، راه‌های مقابله با ویروس‌های کامپیوتری. (۱۳۸۳).

ـ دنینگ، دی. ای، جنگ اطلاعات و امنیت. پژوهشکده پردازش هوشمند علائم، تهران، انتشارات موسسه فرهنگی هنری پردازش هوشمند علائم ۱۳۸۳.

ـ سیدمفیدی، کاوه، (۱۳۸۵)، جنگ سایبری تهران، انتشارات دانشکده امام باقر علیه‌السلام، ۱۳۸۳.

ـ صدوقی، مردادعلی، (۱۳۸۴) تکنولوژی اطلاعاتی و حاکمیت ملی،دفتر مطالعات سیاسی و بین‌المللی، تهران.

ـ طیب، علی‌رضا، (۱۳۸۴) تروریسم: تاریخ، جامعه‌شناسی،گفتمان، حقوق، نشرنی،تهران.

ـ عبدالله خانی، علی، (۱۳۸۰) تروریسم شناسی، مؤسسه فرهنگی و تحقیقات بین‌المللی ابرار معاصر، تهران.

ـ علوی، پرویز ؛مقاله ساخت جهانی اطلاعات درکشورهای شرقی و جنوب شرقی آسیا نوشته چانگ چوانگ یانگ (chung-chung yang) انتشارات ثانیه، تهران،۱۳۸۵.

ـ محبی، جمشید، کارگاه عملیات روانی در فضای سایبری، بهمن ۸۹، سپاه علی بن ابی‌طالب علیه‌السلام

رادیو دویچه وله، خبری با عنوان «القاعده: استفاده از شبکه اینترنت برای عملیات تروریستی»، ۲۰۰۷/۷/۵، موجود برروی سایت www.dw-world.de/dw/article/0,,2671204,00.html

ـ عبدی کلانتری، گزارش گر دویچه وله در نیویورک، «القاعده در اینترنت»، ۸۷/۱۰/۱۵، موجود بر روی سایت www.tor.cn/dw/article/0,,3060047,00.html

ـ مقاله رادیو زمانه با عنوان «آمریکا به دنبال شکار تروریست در اینترنت»، تاریخ ۸۶/۱۲/۱۷ موجود بر روی سایت: www. Radiozamaneh. Com

ـ اعترافات ترورکننده شهید مسعود علی محمدی پخش‌شده توسط صداوسیما ج.ا.ا. در اخبار ۲۰:۳۰ شبکه دوم در مورخه ۸۹/۱۰/۲۲

ـ سایت پژاک در تاریخ ۱/۱۱/ ۸۶ موجود بر روی آدرس: http://pjak.blogsky.com

ـ خبری با عنوان «گسترش نفوذ القاعده در اینترنت، القاعده درصدد گسترش نیروهای خود در حوزه اینترنت و اطلاع‌رسانی است.» تاریخ۱۸/۷/۸۴ موجود بر روی سایت :www.asia-newspaper.ir

ـ گزارش کنل فلتر ریاست مرکز مبارز با تروریسم در اولین جلسه در دهمین کنگره با عنوان «اینترنت دروازه‌ای به‌سوی افراطی‌گری اسلامی خشونت‌بار می‌گوید که فیلم‌هایی از حمله به‌نظامیان آمریکایی پخش می‌گردد.»

منابع انگلیسی

- Joseph H. Felter, The Internet: A Portal to Vilent Islamist Extremism, May 3 2007,
- http://www.mojahedin.org/pages/clips.aspx
- www.hamshahrionline.ir/News/?id=4820
- Cyber War: Espionage of the Internet(jeanguisnel)
- Clay Wilson, Computer Attack and Cyber Terrorism:Vulnerabilities and Policy Issues for Congress, CRS Report for Congress Received through the CRS Web,Order Code RL32114, 2003.
- Pollitt, Mark M., "Cyberterrorism – Fact or Fancy?" Internet. Available: www.cs. georgetown. edu/~denning/infosec/pollitt.html, April 2002.
- Krasavin, Serge Ph.D., What is Cyber-terrorism? SANS Institute available:http:// rr. sans. org/ hackers/terrorism.php, 2002.
- Paul, Larisa, "When Cyber Hacktivism Meets Cyberterrorism." Internet. (February 19, 2001) SANS Institute.available:http://rr.sans.org/hackers/terrorism.php, 2002.
- Elaine, Hanna, "JIHADISM ONLINE :A STUDY HOW AL- QAIDA AND RADICAL ISLAMIST GROUPS USE THE INTERNETFOR TERRORIST PURPOSES", Forsvarets ForskningsINSTITUTT(FFI), Norwegian defence research establishment,p 30,2006
- Elaine Sciolino, "From Tapes, a Chilling Voice of Islamic Radicalism in Europe," The New York Times, November 18 2005
- Audrey Cronin, Behind the Curve, Globalization and International Terrorism, prepublication draft. 2003,
- Robert Windrem, 9/11 Detainee: Attack Scaled Back. September 21, 2003 [http://www. msnbc. com/news/969759.asp.]
- Simson, Garfinkel, Spafford, Gene, and Schwartz, Alan, "Practical Unix and Internet Security", ۳rd Edition, Cambridge, Ma:OReilly and Associates,۲۰۰۳.
- Giampiero Giacomello, "Measuring digital wars: Learning from the experience of peace research and arms control", The Information Warfare.
- Simonis, Ingo, "SENSOR WEBS: A ROADMAP", Institute for Geoinformatics, University of Muenster, Germany.
- Chu, Xingchen, Buyya, Rajkumar, "Service Oriented Sensor Web", Grid Computing and Distributed Systems Laboratory, Dept. of Computer Science and Software Engineering, The University of Melbourne, Australia.
- Lionel M. Ni, Yanmin Zhu, Jian Ma, Minglu Li, Qiong Luo, Yunhao Liu, S.C. Cheung, Qiang Yang, "Semantic Sensor Net: An Extensible Framework", Department of Computer Science Hong Kong University of Science and Technology and Department of Computer Science and Engineering Shanghai Jiao Tong Universit, China.
- www.hawzah.net/fa/MagArt.html?MagazineID=0...6112
- www.hawzah.net/fa/ArticleView.html?ArticleID=77949...7779
- www.irdc.ir/fa/content/8130/default.asp

- ravi-bidar.persiangig.com/document/soft%20war.pdf
- panjerehweekly.com/1389/8/29/MainPaper/69/Page/12/
- www.hozeyeshahidbakeri.com/.../64-2011-09-26-09-52-38.htm
- http://jang-narm.com/index.aspx?siteid=51&pageid=3129&newsview=16365