تهدیدات سایبری و مفهوم سایبر تروریسم

مجتبی جعفری

دانش آموخته کارشناسی ارشد علوم سیاسی، داشنگاه آزاد اسلامی واحد زنجان

استان آذربایجان شرقی، تبریز

Jafari.mojtaba62@gmail.com

چکیده

جهان مدرن امروز با تمام فناوری های چالش برانگیزش انسان را در دو راهی نیستی و هستی قرار داده است. وابستگی انسان به فناوری های نوین ارتباطاتی مانند اینترنت در حال افزایش است، و ارائه خدمات و اجرای امور امنیتی و دفـاعی بـا شـیوه هـای قدیمی هر روز بیش از پیش جای خود را به روش های نوین در زمینه اطلاعات و ارتباطات می دهند. این وابستگی تکنولـوژیکی، جدا از مشکلات گریز ناپذیر فرهنگی و اجتماعی که به دلیل ماهیت فناوری در جوامع مختلف بوجود آورده، از نظرگاه دیگری نیز برای دولت‌ها و شهروندان تحت حاکمیت آن‌ها مسئله ساز شده است. به واقع، در کنار امکانات بیشماری که فناوری اطلاعـات و ارتباطات برای بشر فراهم نموده، تهدیداتی را نیز موجب شده، که احتمال حملات جنگ افروزانه و رفتارهای مجرمانه با استفاده از این فن آوری را تشدید کرده است.

سایبر تروریسم، لزوما یک مرز تفکر برانگیز جدید نیست. با این وجود امروزه این مفهوم بیش از گذشته برجسـته تـر بـه نظـر می‌رسد. سایبر تروریسم به ابزار نوینی برای از بین بردن ساختار های اقتصادی، سیاسی و اجتماعی تبدیل شده است. هم اکنون سایبر تروریسم به صورت تهدید برجسته و معقول برای کشور عزیزمان ایران و نظام مقدس جمهوری اسلامی به شمار می آیـد. سایبر تروریسم تنها برای ویرانی و آسیب رسانی در سطح ظاهری نیست. تهدیدات سـایبری را مـی تـوان در متلاشـی کـردن موقعیت های اقتصادی و زیرساخت های عملیاتی، در زمینه های مدیریت منابع مالی، کمیسیون هـای انـرژی، منـابع امنیتـی و نظامی، حمل و نقل، امکانات بهداشتی، بانکداری، بازرگانی و صنعت، و خدمات حیاتی دیگر، موثر دانست. باید اذعان داشـت کـه تاثیرات این گونه حملات به زیرساخت های حیاتی یک کشور، زمینه های فلج شدن جامعه از لحاظ روانی، فیزیکی و اقتصادی را مهیا می کنند. در این مقاله سعی بر آن است که تهدیدات ممکن در زمینه سایبر تروریسم مورد تحلیل و بررسی قرار بگیرد.

کلمات کلیدی:

فضای سایبری، سایبر تروریسم، تهدیدات سایبری

۱- آغاز سخن

جهان در دهه ۱۹۷۰ میلادی با یک انقلاب تکنولوژیک جدید روبرو شده است. این انقلاب جدید به نام" انقلاب اطلاعات " شهرت یافته است. و همان طور که می دانیم، ماهیت علوم را اطلاعات تشکیل می‌دهد؛ عنصری که به دلیل اهمیت فوق العاده اش، عصر حاضر به آن نام گرفته است [۱]. به خصوص بعد از سال ۱۹۹۰ در سایه اپیدمی فراگیر اینترنت، امنیت ملی کشورها از هر جهت در معرض تهدید قرار گرفته است. به سبب شرکت‌های بین‌المللی، سیستم های گمرکی و بواسطه هکرها، اسرار مخفی دولت و همین طور با رشد قارچ گونه ی سایت‌های غیر قانونی در اینترنت، زندگی واقعی و فضای مجازی (سایبری) و قوانین اجرایی نظام‌های حقوقی در معرض تهدید قرار دارند. خصوصا، تاسیسات زیربنایی و ارتباطاتی شهرهای بزرگ نیز در تیررس چنین تهدیدی هستند.

با پذیرش جهانی اینترنت و فضای مجازی (فضای سایبر)، مفهوم مکان از یک دیدگاه مشخصی کنار گذاشته شده است، ارتباطات بین قاره ای و انتقال اطلاعات با یک اشاره بر صفحه کلید رایانه‌ها امکان پذیر می باشد.

باید به این نکته هم توجه کرد که عامل مهمی که توانست در این پیشرفت پر شتاب، به رایانه کمک شایسته ای کند و قابلیت‌های آن را به شکل مؤثرتر و کارآمدتر در معرض بهره‌برداری گسترده‌ای قرار دهد، ارتباطات الکترونیکی[1] است. پیش از این، بهره‌برداری از سیستم‌های رایانه ای به همان محل استقرار شان محدود می‌شد و همین مسئله به طور چشمگیری از کارآیی شان کاسته بود. اما ارتباطات الکترونیکی امکان دسترس و بهره‌برداری دوردست از سیستم‌های رایانه‌ای را فراهم کرده است، تا آن جا که شبکه‌های رایانه‌ای بزرگ بسیاری در سراسر جهان راه اندازی شده‌اند و اکنون بدون هیچ گونه محدودیت زمانی و مکانی و با کیفیت مطلوب، به ارائه انواع خدمات رایانه ای می پردازند[۲].

پیشرفت تکنولوژیک اینترنت در هر حالی که مزایای قابل توجهی برای جوامع جهانی در بر داشته است، برای گروه های تبهکاری و تروریستی به عنوان ابزاری برای رسیدن به اهداف خود در آمده است و به قولی مفهوم کلاسیک جرم را تغییر داده و جرایم نوینی را به وجود آورده‌اند[۳].

گروه های تروریستی با تهدید امنیت داخلی کشورها و رسیدن به اهداف خود به هر قیمتی، به کمک تکنولوژی رایانه به طور غیر باوری تحرک یافته و به ترافیک بین المللی جرم ، مفهوم جدید بخشیده‌اند.

تکنولوژی رایانه و اینترنت به عنان نماد تاریک جهانی سازی، آرامش اجتماعی و صلح و امنیت ملی مان را به طور جدی در معرض تهدید قرار می‌دهد. تخریب سایت های نهادهای مهم دولتی توسط "هکرها" در قرن بیست و یکم، جرایم رایانه‌ای[2] را به عنوان یکی از انواع دیگر جرم‌ها در موقعیت مهم و غیر قابل انکاری قرار داده است[۴].

سایبر تروریسم یکی از انواع جرایم رایانه ای است که در واقع به معنی استفاده از رایانه‌ها برای رسیدن به اهداف از پیش تعیین شده ی سیاسی و اجتماعی به منظور آسیب به افراد و زیرساخت های اساسی کشور تعبیر می شود. سایبر تروریسم را همچنین می‌توان در مفهوم کلاسیک، انجام فعالیت های تروریستی از طریق رایانه‌ها و سیستم های رایانه‌ای تعریف کرد.

در قانون ضد تروریسم انگلستان در سال ۲۰۰۰، سایبر تروریسم به معنی تحت تاثیر قرار دادن حکومت و یا ترساندن جامعه از طریق نفوذ غیر مجاز به سیستم‌های الکترونیک و یا تخریب آن‌ها است. با توجه به این قانون اگر یک گروه خرابکار به پست الکترونیک نخست وزیر نفوذ کنند و موجب اختلال در سیستم‌های رایانه‌ای گردند، می‌توان به آن نام تروریسم را داد[۵].

یکی از بهترین ابزارها که به نظر می‌رسد تمامی ویژگی‌های مورد نیاز تروریست‌ها را در خود جمع کرده، فضای سایبری است. این مقاله در پی تبیین مفهوم و ماهیت فضای سایبری و ارتباط آن با تروریسم یا به اصطلاح سایبر تروریسم است. در این زمینه، بخش اول به روش تحقیق اختصاص دارد. در بخش دوم، مفهوم و ماهیت فضای سایبری و سایبر تروریسم تبیین می گردد. سپس در بخش سوم به تهدیدات سایبری و تروریسم در فضای سایبری (سایبر تروریسم) خواهیم پرداخت.

[1]. Electronic Communication

[2] . Cyber Crimes

بخش اول. روش تحقیق

- پرسش اصلی

با توجه به مطالب مذکور مسئله‌ای که حائز اهمیت است توضیح و تبیین ماهیت فضای سایبری و سایبر تروریسم و بررسی چگونگی ارتباطشان با یکدیگر می باشد. بر این اساس پرسش اصلی مقاله حاضر این است: آیا وجود تروریسم در فضای سایبری و رسیدن به مفهوم سایبر تروریسم به عنوان تهدید سایبری امکان پذیر است؟ و تهدیدات شناخته شده ی سایبری به چه شکلی معرفی می شوند؟

- گمانه اصلی

در پاسخ به سوال اصلی این مقاله گمانه اصلی ما این است که بر اساس شواهد بدست آمده، تروریسم نوینی در فضای سایبری شکل گرفته است و روز به روز به ابعاد آن افزوده می‌شودکه امنیت ملی را تهدید می‌کند. در این فرضیه، تهدیدات سایبری در رابطه با سایبر تروریسم به عنوان متغییر مستقل و فضای سایبری و امنیت ملی، به عنوان متغیر وابسته در نظر گرفته شده است.

- هدف پژوهش

هدف مقاله حاضر بر هدف زیر مبتنی است :

بررسی دقیق مفهوم و ماهیت فضای سایبری و تهدیدات سایبری سایبر تروریسم و تبیین رابطه ی آنها بایکدیگر می‌باشد.

- روش پژوهش

برای اثبات فرضیه اصلی، روش تحقیق در مقاله حاضر مبتنی است بر:

الف – روش گردآوری داده‌ها به روش کتابخانه‌ای بوده و از بانک‌های اطلاعاتی، فیش برداری از کتب و از مقالات موثق اینترنتی هم استفاده شده است.

ب – نحوه بازگویی و توضیح همبستگی داده‌ها نیز با استفاده از استقرا، استدلال و تحلیل اسناد (Facts)، با روش تحلیلی و توصیفی می‌باشد.

بخش دوم. مفهوم و ماهیت فضای سایبری و سایبر تروریسم (تهدیدات سایبری)

سایبر تروریسم در واقع به تروریسم در فضای سایبری اشاره دارد. تحول در تکنولوژی های ارتباطی به ویژه پیدایش فضای سایبری به خصوص اینترنت به همراه گسترش شبکه‌های رایانه‌ای فرصت های قابل توجهی را برای اعمال افراطی بنیادگریان و گروه های تروریستی فراهم نموده است. ما در برابر مفهوم سایبر تروریسم باید به تلاقی دو مفهوم تروریسم و فضای سایبری دقت بیشتری داشته باشیم. بنابراین برای تبیین بهتر و علمی تر مفهوم سایبر تروریسم در ابتدا باید به طور مجزا به بررسی ماهیت تروریسم و فضای سایبری بپردازیم.

تعریف لغوی واژه ی ترور

داریوش آشوری در کتاب « دانشنامه سیاسی » در توضیح واژه « ترور » می‌نویسد : « ترور در لغت فرانسه به معنای هراس و هراس افکنی است و در سیاست به کارهای خشونت آمیز و غیر قانونی حکومت‌ها برای سرکوبی مخالفان خود و ترساندن آنها به کار می‌برند، ترور می‌گویند و نیز کردار گروه های مبارزی که برای رسیدن به هدف‌های سیاسی خود دست به کارهای خشونت آمیز و هراس انگیز می‌زنند « ترور» نامیده می‌شود. بنا به این تعریف، ترور و تروریسم روشی است که هم حکومت‌ها و هم گروه‌های سیاسی مخالف حکومت برای هراس افکنی و ترساندن طرف مقابل به کار می‌گیرند. ترور به معنای کشتار سیاسی به کار می رود و کسانی را که به کشتار سیاسی دست بزنند ترور گر (تروریست) می‌خوانند [۶].

تعریف فضای سایبری

از لحاظ لغوی در فرهنگ های مختلف سایبر به معنی مجازی و غیر ملموس می باشد. فضای سایبری محیطی است مجازی و غیر ملموس موجود درفضای شبکه های بین المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طور کلی هر آنچه در کرهٔ خاکی به صورت فیزیکی ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران می‌باشند و به طریق کامپیوتر، اجزا آن و شبکه های بین المللی به هم مرتبط می باشند[۷].

فضای سایبری یا مجازی عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می شود. به نظر می رسد به کارگیری این

اصطلاح برای ارجاع به امور فنی، بـه آن رنـگ و بـویی صـرفاً فنـی و مکانیکی داده باشد[۸].

واژه سایبر از لغت یونانی (Kybernetes) به معنی سکاندار یا راهنما مشتق شده است. نخستین بـار ایـن اصـطلاح "سـایبرنتیک" توسـط ریاضیدانی به نام "نوربرت وینر"[3] در کتابی بـا عنـوان "سـایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ به کـار بـرده شـده اسـت. "سـایبرنتیک" علـم مطالعـه و کنتـرل سـاخت‌هـا در سیستمهای انسانی، ماشینی (و کامپیوتر ها) است[۹].

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون[4] نویسنده داستان علمی تخیلی در کتاب نورومنسر[5] در سال ۱۹۸۴ به کار بـرده اسـت. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌هـا از طریق کامپیوتر و مسائل مخابراتی بدون در نظـر گـرفتن جغرافیـای فیزیکی گفته می‌شود. یک سیستم آنلاین نمونـه‌ای از فضـای سـایبر است که کاربران آن می‌توانند از طریق ایمیل با یکـدیگر ارتبـاط بـر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیـاز بـه جابجـایی های فیزیکی نیست و کلیه اعمـال فقـط از طریـق فشـردن کلیـدها یاحرکات ماوس صورت می‌گیرد. این عدم جابجایی فیزیکی، محققان را وا داشـت کـه بـه مطالعـه برخـی شـباهت‌هـای فضـای سـایبر بـا حالت‌های نا هشیاری، بخصوص حالت‌های ذهنـی‌ای کـه در رویـاهـا ظاهر می‌شوند، بپردازند[۱۰].

ماهیت فضای سایبری

فضای سایبری یک نـوع اجتمـاع و همسـایگی بزرگـی اسـت کـه میلیون ها رایانه و کـاربران آن را در سراسـر جهـان بـه هـم مـی پیوندد. با غلبه اینترنت بر زندگی روزانه ی انسان هـا طبیعـی بـه نظر می‌رسد که بسیاری از مشخصه‌های جامعـه سـنتی بـه درون اینترنت کشیده شوند و در آتجا شکل گیرتد. امروزه، فعالیت های بسیاری از زیرساخت‌های حیاتی هر کشوری به تکنولوژی رایانه و فضای مجازی وابسته است. از این رو هیچ جای تعجبی نیست که سایبر تروریست‌ها در فضای مجازی مرتکب اعمال خشونت آمیـز از پیش برنامه‌ریزی شده شوند. به خصوص گمنامی ایـن فضـا بـر گسترش این نوع اعمال خرابکارانه دامن می‌زند، در این فضا کمتر هویت واقعی مشخص می‌شود و افراد با کتمان هویت خـویش بـه راحتی مرتکب انواع جرائم می شوند[۱۱].

برای روشن‌سازی این مفهوم و ارائه تعریفی مناسب باید صفات ذاتـی این پدیده را بیان داشت. مفهوم سایبر فقط به کار اینترنـت محـدود نمی‌شود و تمام روابط اجتماعی که فنآوری‌های اطلاعاتی و ارتباطی[6] در آن بکار رفتـه را شـامل مـی شـود. از سیسـتم ثبـت کـامپیوتری، سیستم‌های سـخنگوی اتوماتیـک و کـارت‌هـای هوشـمند را شـامل می شود[۱۲]. به علت شمول زیاد تسهیلات دیجیتالی برای کالاهـای متعدد مانند کفش های شمارنده قدم و مایکروفر باید عنصـر زنـدگی مجازی موقت را نیز به تعریف اضافه کنیم. تعریف فضای سایبری بـه عنوان فضای میان سخت افزارهای پیشرفته با انسان هرچنـد مـرتبط با زندگی اجتماعی وی باشد مقصود مـا را بـرآورده نمـی سـازد. زیـرا حقوق بشر در روابط میـان دولـت و شـهروندان از اهمیـت بیشـتری برخوردار است تا حقوق بشر در ارتبـاط بـا انسـان و ماشـین هـا، لـذا منظور ما از فضای سایبری فضای موجود میـان انسـان و ماشـین در مواردی است که دولت در کارکرد آن ماشین دخالت دارد و یا موظف به دخالت است. بهترین مصداق چنین فضایی، فضای موجود در میان رسانه های جمعی مانند فـاکس، موبایـل، مـاهواره و اینترنـت اسـت. تفاوت بارزی که میان اینترنت و مـاهواره بـا دیگـر وسـایل ارتبـاطی وجود دارد وجود فناوری راه گزینی بسـته ای[7] در اینترنـت و مـاهواره است. این فناوری به اطلاعات موجود در اینترنت و ماهواره این اجازه را می دهد که بدون توجه به مبدأ به مقصد خود برسند در حالی کـه در دیگر رسانه ها با کمک فناوری مداری[8]، اطلاعات تنها از یک مسیر عبور می کنند[۱۳]. اما تفاوت بنیادین اینترنت با مـاهواره در ویژگـی انباشتگی[9] اطلاعات است. در حالی که اطلاعات در مـاهواره یکسـویه است، اینترنت به علت ویژگی فعل و انفعالی[10] این قابلیت را داراسـت کـه افـراد بـا منـافع مشـترک بتواننـد بـه یکـدیگر ملحـق شـوند و مجموعه ای قدرتمند را تشکیل دهند[۱۴]. این ویژگی در کنار دیگـر ویژگی‌های اختصاصی اینترنت آن را تبدیل به دنیای متفـاوتی کـرده است که حقوق مختص به خود را می طلبد. مقصود ما نیـز از کـاربرد فضای مجازی همین است.

[3]. Norbert Wiener
[4]. William Gibson
[5]. Neuromancer

[6]. ICT
[7]. Packet switching technology
[8]. Circuit switching technology
[9]. aggressive
[10]. interactive

فضای سایبری آخرین مرز الکترونیکی امکانپذیر بشر است که جهان واقعی را تبدیل به مستعمره می‌کند[۱۵]. صحبت از حکمرانی مستقلی در این فضاست. حکومتی بدون سرزمین و بدون جمعیت اما اثرگذار بر دنیای واقعی. فضای مجازی محل ذخیره و تبادل اطلاعات به صورت صفر و یک است که میزانی از زندگی بشر را به خود وابسته کرده است و اختلال در آن می تواند موجب لطمه به حقوق مکتسبه آنها شود. هرچند ریشه اینترنت فعلی در وزارت دفاع امریکا و به عبارتی در مدرنیسم بوده و بعداً توسط شرکت های تجاری بزرگ رشد یافت اما حرکت آن به سمت پست مدرنیسم است. مسیری که در آن شاهد تعریف جدیدی از بشر در آن چارچوب خواهیم بود. اصطلاح بشر مجازی یا شهروند مجازی[11] از جمله تعابیری است که برای این نوع بشر به کار رفته است. اینکه حقوق شهروندی این بشر مجازی چه تفاوتی با نوع سنتی آن دارد در پاسخ به سؤالات بعد روشن خواهد شد.

به طور خلاصه نه موضوع شهروند مجازی به موضوع شهروند سنتی که افراد بودند محدود می‌شود و نه محمول شهروند مجازی به تأثیراتی محدود می شود که توسط افراد قابل بروز بود. مرزها در قرن بیست و یک در حال فروپاشی است؛ در این فضا برخی دولت‌ها علاوه برجنگ، به جرم و تروریسم دست می زنند در حالی که افراد علاوه بر جرم و تروریسم به جنگ نیز دست می زنند. این تحول تا جایی است که برخی کشورها در حال تربیت سربازان مجازی هستند[۱۶]. دلیل تمام این تفاوت ها در ویژگی خاص این فضا نسبت به ایستگاه های سخن‌پراکنی قدیمی است.[12]

ویژگی های فضای سایبری

۱- **جهانی و فرامرزی بودن:** ویژگی منحصر به فردی که فضای سایبری را از دیگر رسانه‌ها جدا می‌سازد، همین برد جهانی است. این جهانی بودن با ارسال گستره امواج ماهواره ای از یک نقطه خاص به سراسر جهان متفاوت است. علاوه بر محدودیت های خاص امواج ماهواره‌ای در مناطق مختلف و مشکلات فنی و محیطی آن، برنامه‌های ماهواره‌ای در یک نقطه مخصوص تولید و سپس انتشار می‌یابد. در حالی که در محیط مجازی اینترنت، امکان تولید جهانی فراهم است[۱۷].

۲- **ویژگی فوق تصور دیگر در فضای سایبری:** امکان ارتباط دو طرفه به صورت سهل و آسان است. به عبارتی در این محیط امکان های خاصی ارتباط سریع و آسان کاربران، سرورها و مدیریت کنندگان را امکان پذیر می سازد این ویژگی نیز در انواع دیگر رسانه‌ها با محدودیت‌ها و مشکلات خاصی رو به روست.

۳- **جذابیت و تنوع، ویژگی دیگر فضای سایبری است:** ضمن اینکه امکان بهره برداری از همه جذابیت های خاص رسانه ای مانند: فیلم، عکس و ...همان طور که ذکر شد مشتری مداری محض در تنوع و جذابیت این محیط تأثیر به سزایی دارد.

۴- **مخاطب خاص و تأثیرگذار:** همین مسأله باعث شده که اینترنت و فضای سایبری نوعی مرجعیت فکری-سیاسی را برای کاربران ایجاد نماید. گرچه می توان ادعا کرد این امر در جوامعی با فراگیری کاربران، موضوعیت خود را تا حدودی از دست داده است. اما حداقل در ایران هم چنان به عنوان یک نقش برای فعالین این عرصه تعریف می شود.

۵- **مسأله دیگر امکان عبور و عدم تقید به بخش مهمی از قوانین و محدودیت های رایج در سایر رسانه‌ها است:** این امر به ویژه در محیط های غیررسمی بیشتر رایج است. به عنوان مثال وبلاگ‌ها با گستردگی میلیونی خود توانسته اند مخاطبانی فراگیر جذب کنند که به طور معمول مقید به قوانین خاصی نیستند و چه بسا وبلاگی با مخاطبانی به مراتب بیشتر از یک وب سایت و خبرگزاری رسمی، با دستی باز همه خطوط قرمز یک جامعه را زیر پا بگذارد و بتواند از سد فیلترینگ و محدودیت های فنی هم رها شود(Girard, 2011:398).

سایبر تروریسم چیست؟

در واقع سایبر تروریسم به معنی استفاده از رایانه ها برای رسیدن به اهداف از پیش تعیین شده ی سیاسی و اجتماعی به منظور آسیب به افراد و زیرساخت های اساسی کشور تعبیر می شود.

[11] . netizen, cybercitizen, global humanity

[12]. این ویژگی‌ها شامل گمنام(anonymity) ، آسانی(easier) ، ارزانی (inexpensive)، جهان‌وطنی(cosmopolitan) ، کنش‌واکنشی (interactive) و فرهنگ یکپارچه (single-culture) می‌شود.

سایبر تروریسم را همچنین می توان در مفهوم کلاسیک، انجام فعالیت های تروریستی از طریق رایانه ها و سیستم های رایانه ای تعریف کرد[۱۸].

واژه سایبر تروریسم نخستین بار از سوی کالین باری[۱۳] و در دهه ۱۹۸۰مطرح شد، ولی گفته می‌شود جامع ترین تعریف از سوی خانم دوروتی دنینگ استاد علوم رایانه‌ای دانشگاه جرج تاون ارائه شده است: سایبر تروریسم حاصل تلاقی تروریسم و فضای مجازی است. سایبر تروریسم بیشتر به معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آنهاست، هنگامی‌که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی و اجتماعی خاص اعمال می شود . در تروریسم کلاسیک مواد منفجره و سلاح‌های گرم اصلی ترین ابزار تروریسم کلاسیک هستند، ولی محتمل ترین ابزار سایبر تروریست ها رایانه است. در واقع آنها ترجیح می‌دهند به جای بمب از بایت[۱۴] استفاده کنند. اساسی ترین روش های سایبر تروریسم عبارتست از: هک کردن، ویروس‌های رایانه ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات[۱۹].

همانطوری که اشاره شده خانم دوروتی دنینگ تعریفی در مورد سایبر تروریسم ارائه داده که به شرح مقابل است: «سایبر تروریسم همگرایی و تقارب تروریسم با فضای مجازی است. و اغلب به معنی حمله و تهدید به وسیله یا علیه کامپیوترها، شبکه‌ها و اطلاعات ذخیره شده برای ترساندن و اجبار و فشار بر یک حکومت و مردمش برای رسیدن به اهداف سیاسی و اجتماعی است. برای واجد شرایط شدن یک حمله به صورت سایبر تروریسم آن حمله بایستی دربرگیرنده خشونت علیه مردم یا دارایی آنها باشد یا حداقل منجر به بازتولید وحشت و ترس گردد. این تعریف حملاتی که منجر به مرگ یا جراحت بدنی، انفجار، سقوط هواپیماها، آلودگی هوا یا کاهش قدرت اقتصادی یا سقوط اقتصادی می گردد را شامل می شود. بر اساس اثراتی که حملات سایبرتروریستی دارند می توان گفت که حمله به زیرساخت‌های اساسی جلوه هایی از سایبرتروریسم هستند. حملاتی که سرویس‌ها و خدمات غیرضروری را مورد حمله قرار می دهند یا مایه آزار اندک شوند جزء این تعریف نمی شوند»[۲۰].

بخش سوم. تهدیدات سایبری و سایبر تروریسم (تروریسم در فضای سایبری)

دامنه اثر سایبر تروریسم بیشتر است مخصوصاً جوامع پیشرفته غربی که به شبکه های الکترونیکی بسیار وابسته هستند، آسیب پذیری شان در برابر حملات تروریستی، سرقت و خراب کاری در سطح ملی مطرح است. این خطر به گونه ایست که یک مقام امنیتی آمریکا گفته است با یک میلیارد دلار و کمک بیست نفر متخصص خبره رایانه می‌تواند کل آمریکا را فلج کند. یک تروریست هم می‌تواند به این توانایی دست یابد[۲۱].

سایبر تروریست می‌تواند شبکه های دولتی یا رایانه های دولتی، شخصی، خدمات عمومی، خطوط هوایی خصوصی و ... را مورد حمله قرار دهد. تعداد زیاد و پیچیدگی حملات احتمالی به تروریست‌ها کم می‌کند تا نقاط ضعف و آسیب پذیر را برای حمله پیدا کنند.

انسان ها از همان ابتدای هبوط به زمین به دلیل اختلاف سلیقه و اختلاف عقیده دچار تقابل شده اند. ماجرای هابیل و قابیل شاهد این مدعاست، داستانی که تا به امروز ادامه یافته است به گونه ایی که انسان ها گاهی برای ابراز یا به کرسی نشاندن عقیده خود به افراد، سازمان‌ها یا دولت ها، دست به خشونت زده اند (پدیده تروریسم) و بسته به امکانات و تکنولوژی بشر در هر عصر از ابزارهای متفاوتی استفاده کرده اند. با ورود اینترنت به عرصه تعاملات اجتماعی، سیاسی و اقتصادی بشر، مفهوم تروریسم هم تفسیر و ابزار جدیدی پیدا کرد و پدیده‌ای به نام سایبر تروریسم متولد شد. ما در این بخش به معرفی ویژگی ها و شیوه های این پدیده می‌پردازیم و بیان خواهیم کرد که سایبر تروریست‌ها چگونه و به چه وسیله‌ای و به خاطر چه اهدافی دست به این اقدامات می‌زنند و چه عواملی در بروز و تشدید آن موثر است؟ [۲۲].

همان طور که مواد منفجره و سلاحهای گرم، اصلی ترین ابزار تروریسم کلاسیک هستند. محتمل ترین اسلحه سایبرتروریست‌ها نیز رایانه است. روش های زیادی وجود دارد که تروریست ها می‌توانند از رایانه به عنوان یک وسیله تروریستی استفاده کنند. اساسی ترین روشهای سایبر تروریسم عبارتند از : هک کردن و ویروس های رایانه ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات.

دلایل زیادی وجود دارد که سبب می‌شود سایبر تروریسم برای تروریست‌ها جذاب باشد از جمله[۲۳]:

[13]. Collin Barry

[14]. Byte

۱- سایبر تروریسم ارزان تر از روش‌های تروریستی متداول (کلاسیک) است. تنها چیزی که نیاز است یک رایانه شخصی متصل به اینترنت است. نیازی به خرید اسلحه نیست. می‌توان ویروس‌های رایانه را ساخت و از طریق خطوط تلفن، کابل و ارتباط بی سیم آن را ارسال کرد.

۲- سایبر تروریسم ناشناخته تر از روش‌های تروریسم کلاسیک است. مانند بسیاری از کاربران اینترنت، تروریست‌ها از اسامی‌مستعار استفاده می‌کنند و به یک سایت به عنوان کاربر مهمان و ناشناس وصل می‌شوند و برای نیروهای پلیس و امنیتی بسیار سخت است که هویت واقعی آنها را ردیابی کنند. در فضای مجازی هم موانع فیزیکی مانند ایست بازرسی، مرز یا گمرک وجود ندارد.

۳- تنوع و تعداد حملات بسیار زیاد است. سایبر تروریست می‌تواند شبکه‌های دولتی یا رایانه‌های دولتی، شخصی، خدمات عمومی، خطوط هوایی خصوصی و ... را مورد حمله قرار دهد. تعداد زیاد و پیچیدگی حملات احتمالی به تروریست‌ها کمک می‌کند تا نقاط ضعف و آسیب پذیر را برای حمله پیدا کنند. مطالعات نشان داده است شبکه های برق و خدمات اضطراری در برابر حملات سایبر آسیب پذیر هستند برای اینکه زیر ساخت و سیستم های رایانه که این‌ها را اداره می‌کنند بسیار پیچیده هستند و این موضوع رفع همه نقاط ضعف را غیر ممکن می‌کند.

۴- سایبر تروریسم را می‌توان از راه دور هدایت کرد، ویژگی که جذابیت زیادی برای تروریست‌ها دارد. سایبر تروریسم، آموزش فیزیکی اندکی را می‌طلبد، سرمایه گذاری روانی کمتر و خطر مرگ کمتری دارد و امکان می‌دهد تا سازمان‌های تروریستی عضو گیری کنند و اعضا را در اختیار داشته باشند.

۵- سایبر تروریسم توانایی زیادی دارد تا تعداد زیادی از مردم را به خود جذب کند، از این رو پوشش خبری و رسانه ای بیشتری را ایجاد می‌کند و این همان چیزی است که تروریست‌ها دنبالش هستند.

۶- دامنه اثر سایبر تروریسم بیشتر است مخصوصاً جوامع پیشرفته غربی که به شبکه های الکترونیکی بسیار وابسته هستند، آسیب پذیری شان در برابر حملات تروریستی، سرقت و خراب کاری در سطح ملی مطرح است. این خطر به گونه ایست که یک مقام امنیتی آمریکا گفته است با یک میلیارد دلار و بیست نفر متخصص خبره رایانه می‌تواند کل آمریکا را فلج کند. یک تروریست هم می‌تواند به این توانایی دست یابد. در مواردی تاثیر حمله به شبکه‌های رایانه‌ای از تاثیر بمب شیمیایی و میکروبی بدتر است. از این رو در یک گزارش رسمی، سایبر تروریسم یکی از ۵ تهدید امنیتی عمده برای ایالت متحده امریکا دانسته شده است[۲۴].

۷- روش‌های کلاسیک تروریستی اهداف تروریست‌ها برآورده نمی‌کند.

اهداف سایبر تروریسم:

به طور کلی در پی سناریوهای مختلف در رابطه با حملات سایبری به زیرساخت های مهم یک کشور آنها را می توان به طور خلاصه طبقه بندی کرد[۲۵] :

۱) حملات سایبری بر نهادهای رسمی و دولتی
۲) حملات سایبری بر صنعت انرژی
۳) حملات سایبری بر مراحل بازیافت زباله
۴) حملات سایبری بر بخش مالی و اقتصادی
۵) حملات سایبری بر بخش بهداشت
۶) حملات سایبری بر بخش فناوری اطلاعات و ارتباطات
۷) حملات سایبری بر بخش تولید و توزیع مواد غذایی
۸) حملات سایبری بر بخش امنیت عمومی
۹) حملات سایبری بر بخش حمل و نقل

معرفی بزرگترین حملات سایبری جهان

متخصصان امور امنیت رایانه ای در جهان با بررسی پنج نمونه از بزرگترین و جدیدترین حملات سایبری در کشورهای مختلف، کرم استاکس نت را که به شکلی گسترده قصد تحت تاثیر قرار دادن ایران را داشت یکی از پیچیده ترین حملات سایبری جهان می‌دانند[۲۶]. همان طوری که می دانیم ما در جهان مجازی زندگی می کنیم، از بانکداری گرفته تا ارتباطات و یا خرید، تقریبا تمامی فعالیتهای روزانه بشر به سوی اینترنت گرایش یافته است، متاسفانه هرچه بشر بیشتر

بر تکنولوژی تکیه می کند بیشتر در معرض خطر حملات سایبری یا مجازی قرار می گیرد.

شاید بزرگترین نگرانی درباره آنچه افراد مختلف آن را "پنجمین میدان جنگ" می خوانند (چهار میدان دیگر زمین، دریا، هوا و فضا هستند) نامرئی بودن آن است. به دلیل اینکه حملات سایبری از طریق شبکه های پیچیده رایانه ای و معمولا از جانب منابع درجه دو یا سه انجام می گیرند، تعیین منشا اصلی برخی از این حملات تقریبا غیر ممکن است[۲۷].

به گفته "آرون سود" نایب رئیس مرکز بین المللی سایبری در دانشگاه "جورج میسون" اگر یک هواپیما را ببینید می دانید که به نیروی هوایی کشوری تعلق دارد، اما اگر به شما حمله سایبری شود حتی نمی‌توانید بفهمید از کجا به شما حمله شده است[۲۸].

حملات سایبری دامنه متنوعی دارند، از شوخی های معمولی گرفته تا کرم های مخرب رایانه ای که به واسطه حافظه های قابل حمل جا به جا شده و امنیت کلی کشوری را به خطر می اندازند. از آنجایی که امروزه تمامی زندگی ما به تکنولوژی، رایانه‌ها و اینترنت گره خورده است اطمینان از ایمن بودن این ابزارها بسیار حیاتی است.[۲۹].

متخصصان با بررسی حملات سایبری پیشین به بررسی سازه هایی پرداخته اند که بیشترین آسیب پذیری را در برابر حمله های تبهکارانه سایبری داشته اند تا راه حلی مناسب به دست آورند. در اینجا پنج نمونه خبرساز از حملات سایبری را که در میدان جنگ پنجم رخ داده اند نام می بریم[۳۰]:

- کرم استاکس نت-۲۰۱۰
- عملیات آئورا-۲۰۰۹
- فرماندهی مرکزی ایالات متحده آمریکا-۲۰۰۸
- گرجستان- ۲۰۰۸
- استونی-۲۰۰۷

تهدیدات سایبری محتمل در سال ۲۰۱۱[۳۱] :

۱- ساخت بدافزار (Malware Creation): در سال ۲۰۱۰، آزمایشگاه امنیت ضد بدافزار پاندا (Pandalabs) رشد فزاینده ای را در مقدار بدافزارهای کشف شده که در حدود بیش از ۲۰ میلیون در سال ۲۰۰۹ را اعلام داشت.

۲- جنگ سایبری (Cyber War): ویروس استاکس نت (Stuxnet)، افشاگری های (Wikileaks) و حمله سایبری به سایت موتور جستجوس گوگل (Google) از نمونه های جنگ سایبری به حساب می آیند. هدف اصلی ویروس استاکس نت باتوجه به قراین و اسناد منتشر شده، از کار انداختن سانتیفیوژهای غنی سازی اورانیوم در راکتور هسته ای نیروگاه بوشهر بوده است.

۳- اعتراض سایبری (Cyber-protest): اعتراض سایبری یا هکتیویزم (Hactivism)، به صورت یک شورش در حال رشد با بسامدی ادامه دار مورد توجه است.

۴- مهندسی اجتماعی: مجرمان سایبری، از سایت های رسانه های اجتماعی برای جذب اعتماد کاربران اینترنتی به نفع اهداف خود استفاده می کنند. برای نمونه باید به حملات گوناگون به شبکه های اجتماعی معروفی مانند فیس بوک و توییتر اشاره کرد.

۵- بد افزار های نفوذی در ویندوز هفت (Windows 7): حمله ی این بدافزارها حداقل در دوسال اخیر که به طور خاص برای ویندوز هفت طراحی شده اند، رصد شده است.

۶- تلفن های همراه: در سال ۲۰۱۱ امکان حمله های جدید بر روی تلفن های همراه پیش بینی شده بود، اما این حملات در حالت بسیار غیر قابل تصوری نبوده اند.

۷- تابلت‌ها (Tablets): سلطه ی آی پدها (ipad) با رقابت محصولات شرکت های دیگر به چالش کشیده شده است. بنابراین آزمایشگاه امنیتی ضد بدافزار پاندا معتقد نبودند که پی سی های تابلت در سال ۲۰۱۱ در معرض اهداف مجرمان انترنتی قرار خواهند گرفت.

۸- رایانه های Mac (مکینتاش متعلق به شرکت اپل): بدافزارها برای راینه های Mac هم وجود دارند، بزرگترین نگرانی در این مورد وجود حفره های امنیتی در سستم عامل اپل (Apple) است.

۹- زبان رایانه ای HTML5: HTML5 (یک زبان رایانه‌ای که برای تدوین قالب و طراحی صفحات وب) به شکل هدف مهمی برای انواع اعمال مجرمانه و تروریستی در آمده است. آزمایشگاه ضد بدافزار پاندا در انتظار اولین حملات بر روی HTML5 در سال ۲۰۱۱ بود.

۱۰- حملات کاملا پویا و رمزدار: آزمایشگاه ضد بد افزار پاندا در انتظار تهدیدات پویا و رمزار پیشرفته هست. به گمان این آزمایشگاه، تهدیدات بسیاری بر علیه کاربران خاص به ویژه شرکت ها، از طریق سرقت اطلاعات موجب بالا رفتن قیمت‌ها در بازار سیاه خواهند شد.

نمونه های سایبر تروریسم در ایران

در مورد سایبر تروریسم در ایران می توان به یک نمونه عمده و مورد توجه مسئولین و مقامات ایرانی و همین طور رسانه های داخل و خارج از کشور اشاره کرد. که در این مقاله، به طور اجمالی به حمله سایبری ویروس استاکس نت اشاره می کنیم.

متخصصان امنیت شبکه، نرم افزاری به شدت مخرب را که گمان می رود نیروگاه‌ها و سیستم های آبرسانی ایران را مورد هدف قرار داده شناسایی و اعلام کردند که ۶۰ درصد آلودگی های مرتبط با این ویروس در سراسر جهان شبکه های مجازی ایران را هدف قرار داده اند[۳۲].

بر طبق گزارشی، پیچیدگی کرم نرم افزاری استاکس نت[15] به اندازه‌ای است که برخی از متخصصان حدس می زنند ساخت این نرم‌افزار مخرب توسط تروریسم سایبری صورت گرفته باشد. به بیانی دیگر گروه یا کشوری با هدف تخریب ساختارهای حیاتی یک کشور این نرم افزار را نوشته و فعال کرده است. گفته می شود این اولین ویروس رایانه ای است که با هدف ایجاد تغییرات فیزیکی در جهان واقعی ساخته شده است [۳۳].

از این نرم افزار می توان برای برنامه ریزی مجدد دیگر نرم افزارها استفاده کرد تا رایانه‌ها را مجبور کنند دستورهای متفاوتی را به اجرا بگذارند. برخی از متخصصان امنیتی بر این باورند که این کرم رایانه ای برخی از ساختارهای حیاتی کشور ایران از جمله نیروگاه های اتمی این کشور را نیز مورد هدف قرار داده است.

حتی برخی از متخصصان حدس می زنند که این ویروس با هدف ایجاد اختلال و تاخیر در راه اندازی نیروگاه اتمی بوشهر و یا غنی سازی اورانیم در نطنز ساخته شده است. با این همه بسیاری از کارشناسان نیز شواهد موجود را به اندازه ای کافی نمی دانند تا بتوان بر اساس آنها هدف واقعی ساخته شدن چنین ویروس خطرناکی را آشکار کرد[۳۴].

بر اساس گزارش بی بی سی، متخصصان سایمنتک پروژه ساخت چنین ویروس پیچیده ای را پروژه ای عظیم، با برنامه ریزی قوی و پشتیبانی مالی بسیار قدرتمند می دانند. از سویی دیگر یکی از سخنگوهای شرکت زیمنس با بیان اینکه این شرکت ۳۰ سال است که هیچ همکاری با ایران نداشته اعلام کرد هیچ یک از نیروگاه های ایران از نرم افزارهای کنترلی زیمنس استفاده نکرده اند زیرا این نیروگاه‌ها با همکاری یک پیمانکار روس ساخته شده اند[۳۵].

در کل باید اذعان داشت که از عمر پیدایش ویروس استاکس نت تا به حال یک سال می گذرد.و هنوز دلایل محکمی بر ماهیت سایبر تروریستی و یا جنگ سایبری این ویروس وجود ندارد . البته نمی توان تبلیغات وسیع رسانه ای را در بزرگ جلوه دادن خطرات این ویروس نادیده گرفت.

نتیجه‌گیری

پتانسیل تهدید سایبر تروریسم روز به روز در حال افزایش است. تعدادی از متخصصان امنیتی و سیاستمداران، احتمال حمله به زیرساخت های فن آوری بخش مالی، خدمات، غیر نظامی و نظامی در کشورهای توسعه یافته و در حال توسعه مانند ایران را بیان کرده اند.

در دوران مدرن امروز، بزرگترین هراس در کنار نام " سایبر تروریسم " پدید آمده است. ابزارهای فن آوری و وابستگی های مدرن و احساس ترس قربانی شدن به واسطه ی آنها و همچنین عدم امنیت فن آوری های رایانه ای ، وحشت از سایبر تروریسم را به وجود آورده است.

بدون شک مرموز بودن سایبر تروریسم، پتناسیل آسیب رسانی در محیط عمومی، تأثیر روانی و جاذبه ی رسانه ای آن همواره توسط تروریست های مدرن مورد توجه قرار گرفته است. با وجود این ، در امکان ترس سایبری بسیار اغراق می شود. تاکنون از سوی تروریست‌ها نمونه‌ای که وجود حمله ی سایبری جدی بر علیه زیرساخت‌های حیاتی در یک کشور را که بتوان به آن عنوان سایبر تروریسم را داد، هنوز ثبت نشده است. البته باید اشاره کرد که در مورد آسیب رسانی غیر قابل تصور ویروس استاکس نت و حمله به نیروگاه اتمی بوشهر هنوز تردید هایی وجود دارد و امکان تبلیغات روانی رسانه ای را نباید نادیده گرفت.

تجهیزات هسته‌ای، سیستم‌های حساس نظامی و سیستم‌های رایانه‌ای شرکت‌های پیشرفته‌ی جهانی تا حد امکان به بهترین شکل حفاظت می‌شوند. نفوذ به این سیستم‌ها بسیار سخت است. با این وجود، سیستم‌های موجود در بخش خصوصی امنیت کمتری دارند و امکان خطرات احتمالی دارای حساسیت بیشتری است.

[15] . Stuxnet

همواره احتمال اغراق در بزرگ نمایی پتانسیل سایبر تروریسم وجود دارد. با این همه، رد یک تهدید و یا نادیده گرفتن آن اشتباه است. پیروزی در مبارزه با تروریسم متعارف و کلاسیک می تواند تروریست‌ها را به سوی سایبر تروریسم سوق دهد.

جمهوری اسلامی ایران در حد کشورهای پیشرفته هم نباشد باید تهدید سایبر تروریسم را جدی بگیرد. برای این که میزان حفره‌های امنیتی در سیستم‌های رایانه ای در حد قابل تصوری بالا است. در اهداف مورد نظر عناصر تروریستی چه در داخل و خارج، آسیب‌پذری محتمل زیرساخت های حیاتی کشور وجود داشته و خواهد داشت. بنابراین امنیت روزافزون این زیرساخت‌ها باید به شکل علمی و سازمان یافته‌ای برنامه ریزی شده و به اجرا در آید.

منابع

[۱] آنجیلیز ، جینا دی. جرایم سایبر . ترجمه ی سعید حافظی و عبدالصمد خرم آبادی ، دبیرخانه ی شورای عالی اطلاع رسانی ، ۱۳۸۳.

[۲] دزیانی ، محمد حسن. جزوه آموزشی حقوق سایبر و جرایم سایبری . تهران ، ۱۳۸۴.

[3] Anderson, J.Q. and L. Rainie, The future of Internet, Pew Research Center, Washington, D.C., 2010.

[4] Prasad, R.V. (2000), "Hack the Hackers", http://www.hindustantime.com/nonfram/191200/detOPI01.asp,25.09.2011.

[5] Ballard, M., "UN rejects international cybercrime treaty", Computer Weekly, 20 April 2010.

[۶] آشوری ، داریوش. دانش نامه سیاسی . تهران : انتشارات مروارید ، ۱۳۸۲.

[۷] صدیق بنای، هلن، (۸۵/۶/۲۸) همشهری آن لاین، "فضای سایبر چیست؟"، hamshahrionline.ir/news/?id=4820، ۹۰/۷/۵.

[۸] "فضای مجازی"، (۸۷/۱۲/۲۰)، از:Cyber-space.blogfa.com ، ۹۰/۷/۶.

[۹] "فضای سایبر"، (۸۷/۴/۲) همشهری، از: www.hamshahri.org/service-42.aspx، ۹۰/۷/۶.

[۱۰] – "فضای سایبر چیست؟"، (۸۸/۵/۶)، از: www.webopedia.com/TERM/C/cyberspace.html، ۹۰/۷/۶.

[11] Bidgoli, Hossein, the Internet encylopedia, Jhon Wiley&Sons Inc., 2004.

[12] Hamelink, Cees, Human Rights in Cyberspace, (1998), http://www.religion-online.org/showarticle.asp?title=283, 2011/9/10.

[13] Koutouki, Dina, "Human Rights: Benefits of Information Technology", University of New Brunswick Law Journal, No.48, 1999.

[14] Keats Citron, Danniele, "Cyber Civil Rights", Boston University Law Review, Vol.89, 2009.

[15] Alexander, K. B., "Warfighting in cyberspace" Joint Force Quarterly, National Defense University Press, 46(3), 2007.

[۱۶] جلالی فراهانی، امیر حسین، "تروریسم سایبری"، مجله فقه و حقوق، شماره ۱۰، پاییز ۱۳۸۵.

[17] Janczewski, Lech. And Colarik, Andrew, Managerial Guide for Handling Cyber- Terrorism and Information Warfare, Idea Group Publishing, 2005.

[18] Colarik, Andrew Michael, Cyber Terrorism: Political and Economic
Implications, Idea Group Inc., 2006.

[19] Denning, Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", in Networks and Netwars: The Future of Terror, Crime, and Militancy (J. Arquill and D.F. Ronfelt eds.), RAND, 2001.

[20] Walker, Clive, "Cyber-terrorism: Legal Principle and Law in the United Kingdom", Penn State Law Rev., 110, no.3, winter 2006.

[21] Verton, Dan, Black Ice: The Invisible Threat of Cyber – Terrorism, Mc Graw-Hill Companies, 2003.

[22] Linden, Edward V., Focus on Terrorism, Nova Science Publishing, Inc., 2007.

[23] "Reponses to Cyber Terrorism", NATO Science for Peace and Security Series E: Human and societal Dynamics, Vol.34, ISO Press, 2008.

[24] Janczewski, Lech, and Colarik, Andrew, Cyber Warfare and Cyber Terrorism, IGI Global, 2008.

[25] Lewis, J. A., "Assesing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threats", Report Center for Strategic and International Studies (CSIS), Washington D.C., 2002.

[26] Tabansky, Lior, "Basic Concepts in Cyber Warfare", Military and Strategic Affairs, Volume 3, No.1, May 2001.

[27] Clarke, R.A. and Knake, R.K.Cyber War, the next threat to national security and what to do about it. New York: Ecoo/HarperCollins, 2010.

[28] Libicki, M.C., Cyberdeterrence and Cyberwar, RAND Corporation, Santa Monica, 2009.

[29] Davis, J. (2007), "Hackers Take down the Most Wired Country in Europe", http://www.wired.com/politics/security/magazine/75-09/ff_estonia? Currentpage=all, 27.10.2011.

[30] Hern, K., Williams, P., and Mahncke, R. J.,"International Relations and Cyber Attacks: Official and Unofficial Discourse", Australian Information Warfare Security Conference Edith Cown University, 2010.

[31] "Pandalabs Predicts Security Trends for 2011", Press Panda Security, http://www.press.pandasecurity.com, 15.10.2011.

[32] Bond, A., (2010)." Simens Stuxnet attack sophisticated, targated".
http://www.cntrolglobal.com/industrynews/2010/163.html, 17.11.2011.

[۳۳] ثابتی راد ، عباس ، (۸۹/۷/۱۹) همشهری آن لاین، "استاکس نت پیش قراول جنگ سایبری است"، از: http://www.hamshahri.org/news-118092.aspx ، ۹۰/۷/۸.

[۳۴] مرشدی ، ارسلان، (۸۹/۷/۳) تبیان، "تروریسم سایبری فعال شده"، از: http://www.tebyan.net/index.aspx?pid=17257&threadID=235020، ۹۰/۷/۸.

[۳۵] "تروریسم سایبری علیه ساختارهای نیرو گاهی ایران" ، روزنامه جام جم، شماره ۲۹۷۴ ، ۸۹/۷/۲۹.