فصلنامه مطالعات جنگ
سال سوم، شماره دهم، پاییز ۱۴۰۰
مقالهٔ دوم از صفحه ۳۵ تا ۶۱

تاثیر تهدیدات علمی و سایبری بر نیروهای مسلح جمهوری اسلامی و امنیت ملی ایران

حسین کوهساریان(نویسنده مسئول) [۱] محمد تقی پرتوی [۲] محمد اکرمی‌نیا [۳] علیرضا شکیب [۴]

دریافت مقاله: ۱۴۰۰/۰۷/۱۵ پذیرش مقاله:۱۴۰۰/۰۹/۰۱

چکیده

تحقیق حاضر با هدف پاسخگویی به این سوال صورت گرفته است که تهدیدات نرم فرهنگی دشمن چه تاثیری بر توان رزمی نیروهای مسلح جمهوری اسلامی ایران دارد. این تحقیق از نوع کاربردی توسعه‌ای و از نظر روش زمینه‌ای موردی است. پس از بررسی دیدگاه‌های نظری در حوزه تهدیدات نرم فرهنگی و توان رزمی نیروهای مسلح، ابعاد و مولفه‌های آن شناسایی شده و به منظور تعیین میزان تاثیر مولفه‌ها، نسبت به تنظیم پرسشنامه بین جامعه آماری اقدام گردید. ، جامعه آماری این پژوهش شامل اساتید دانشگاه عالی دفاع ملی و فرماندهان سطح استراتژیک نیروهای مسلح بوده که با استفاده از فرمول کوکران تعداد ۸۸ نفر (با مدارک دکتری، حوزوی و کارشناسی) به عنوان حجم نمونه تعیین گردیدند. روش جمع آوری اطلاعات و داده‌ها به روش کتابخانه‌ای و میدانی بوده و با استفاده از ابزارهای پرسشنامه و فیش برداری کتابخانه‌ای، داده‌های لازم جمع آوری گردیده است. داده‌های تحقیق با استفاده از شیوه‌های آماری توصیفی و تحلیل‌های کیفی مورد تجزیه و تحلیل قرار گرفته‌اند. نتیجه تحقیق بیانگر این است که دشمنان برای مقابله با انقلاب اسلامی و ارزش‌های اسلامی و جلوگیری از نفوذ فرهنگی جمهوری اسلامی ایران و تضعیف ارکان اقتدار آفرین جمهوری اسلامی ایران بخصوص تضعیف توان رزمی نیروهای مسلح در حوزه عوامل غیر فیزیکی برتر ساز توان رزمی یعنی شهادت طلبی و ولایت مداری، با ابزارهای مختلف نسبت به عملی کردن اهداف خود، سرمایه گذاری و برنامه ریزی کرده است.

واژگان کلیدی: تهدیدات سایبری، وابستگی علمی، وابستگی نرم افزاری

[۱]- نویسنده مسئول و کارشناس ارشد مدیریت دفاعی دانشکده فرماندهی و ستاد آجا ایمیل: H.Kohsarian@CASU.AC.IR
[۲]- عضو هیئت علمی دافوس آجا ایمیل: mt.partovi@ut.ac.ir
[۳]-استادیار دافوس آجا ایمیل: m.akraminia@iran.ir
[۴]- کارشناس ارشد مدیریت دفاعی دافوس آجا

مقدمه

امروزه فضای تبادل اطلاعات که از آن به عنوان فضای مجازی یا سایبری نام برده می‌شود، همانند زمین، هوا، دریا و فضا به عنوان بخشی از قلمرو حاکمیتی شناخته شده و محافظت و دفاع از آن به منزله دفاع از امنیت ملی کشورها تلقی می‌گردد. در سطح جهان، مباحث سایبری که شامل ایجاد و ارتقای امنیت زیرساخت‌های حیاتی، رسیدگی و مقابله با تهدیدات (حوادث) سایبری و عملیات جاسوسی و دفاعی (آفند و پدافند) می‌گردد به دو بخش کلان حوزه نظامی و غیرنظامی (کشوری) تقسیم می‌گردد. حوزه نظامی مسئولیت محافظت از زیرساخت‌های فناوری اطلاعات نظامی و استفاده از فرصت‌هایی که در فضای سایبر برای اهداف نظامی قابل حصول می‌باشد را در کنار مدیریت جنگ سایبر به عهده دارد.

فضای سایبر: منظور از فضای سایبر یا فضای مجازی ترکیبی از ده‌ها هزار رایانه به هم پیوسته، سرویس دهنده‌ها، شبکه‌های ارتباطی، سوئیچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سامانه جامعه فراهم می‌آورد.

تهدید سایبری: مخاطرات موجود در فضای سایبری را تهدید سایبری گویند. تهدید سایبری یک عامل بالقوه برای نقض امنیت در فضای سایبری است. تهدید سایبری در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش یا رخداد که بتواند در امنیت سایبری رخنه ایجاد نموده، منجر به صدمه شود به وجود بیاید.

جنگ سایبری: استفاده از رایانه‌ها، به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار، جهت ترساندن یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و آرمانی انجام می‌گیرد و مکان‌ها و تاسیسات حیاتی، مانند انرژی، حمل و نقل، ارتباطات، سرویس‌های ضروری را هدف قرار می‌دهد و از شبکه های رایانه‌ای به عنوان بسترهای جهت انجام این اعمال خرابکارانه استفاده می‌کند [1].

حوزه نظامی مسئولیت محافظت از زیرساخت‌های فناوری اطلاعات نظامی و استفاده از فرصت‌هایی که در فضای سایبر برای اهداف نظامی قابل حصول می‌باشد را در کنار مدیریت جنگ سایبر به عهده دارد.

تهدیدات سایبری در حوزه ارتش، باید یک مسئله امنیت ملی تلقی شود که منافع ملی و زیرساخت‌های حیاتی ارتش و کشور را در معرض خطر قرار می‌دهند.

جنگ سایبری ترکیبی از ۶ شکل مختلف جنگ اطلاعاتی به شرح زیر می‌باشد:

۱) جنگ فرماندهی و کنترل: که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن است.

۲) جنگ بر پایه اطلاعات :که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی است، که برای برتری در فضای نبرد در جستجوی دانش، کافی هستند.

۳) جنگ الکترونیک: تکنیک‌های رادیویی، الکترونیک یارمزنگاری .

۴) جنگ روانی: که در آن از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی طرف‌ها و دشمنان استفاده می‌شود.

۵) جنگ هکرها :که در آن به سیستم‌های رایانه ای حمله می‌شود.

۶) جنگ اطلاعاتی اقتصادی: ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات، با هدف کسب برتری اقتصادی.

فضای مجازی بخشی از قلمرو حاکمیتی کشورها شده است و امنیت ملی آن‌ها، شامل دفاع از فضای سایبری نیز می‌شود. اجرای عملیات سایبری نیز یکی از وظایف ارتش جمهوری اسلامی ایران محسوب می‌گردد .لازمه انجام این وظیفه، داشتن قابلیت‌های است. با توجه به بالنسبه جدید بودن این وظیفه، در ابتدا باید قابلیت‌های مورد نیاز آن را شناسایی نماییم تا با کسب آنها آجا بتواند این مأموریت را اجرا کند.

اجرای عملیات سایبری یکی از وظایف ارتش جمهوری اسلامی ایران محسوب می‌گردد، چرا که از یک سو برای محافظت از زیرساخت‌های فناوری اطلاعات و ارتباطات خود باید قادر به دفاع پدافند سایبری باشد و از سوی دیگر به موجب اصل یکصد و چهل و سوم قانون اساسی ارتش جمهوری اسلامی ایران پاسداری از استقلال و تمامیت ارضی و نظام جمهوری اسلامی کشور را برعهده دارد و بر این اساس خواه به عنوان وظیفه اصلی و خواه به عنوان وظیفه فرعی آجا باید قابلیت اجرای عملیات سایبری و استفاده از فضای سایبر برای اهداف نظامی را داشته باشد.

انواع نفوذگران سایبری

نفوذگران در فضای سایبر به طرق مختلف دسته بندی شده‌اند که معروف ترین آنها به شرح ذیل می‌باشند:

گروه نفوذگران کلاه سفید[۱]:

کسی که بتواند ازسد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه ای انجام ندهد را یک هکر کلاه سفید می خوانند. این افراد متخصص شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا و به مسئولان گزارش می‌دهند.

گروه نفوذگران کلاه سیاه[۲]:

اشخاصی هستند که وارد کامپیوتر قربانی خود شده و به دستبرد اطلاعات، جاسوسی و یا پخش ویروس و غیره می‌پردازند.

گروه نفوذگران کلاه خاکستری[۳]:

اشخاصی هستند که وسط دو تعریف بالا می باشند.

گروه نفوذگران کلاه صورتی[۴]:

این افراد آدم‌های کم سوادی هستند که با چند نرم افزار خرابکارانه به آزار و اذیت دیگران اقدام می کنند.

گروه نفوذگران کلاه قرمز[۵]:

عده‌ای متخصص که اطلاعاتی نادرست را به شبکه‌های اینترنت وارد می‌کنند. حملات نفوذگران عمدتاً با قصد و منظور هایی صورت می‌گیرد شامل: شنود که در این روش نفوذ گر می تواند به شکل مخفیانه از اطلاعات نسخه برداری کند، تغییر اطلاعات که در این روش نفوذ گر به دستکاری و تغییر اطلاعات می‌پردازد، افزودن اطلاعات که در این روش نفوذ نفوذ گر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند و وقفه که در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

فنون جنگ سایبری:

فنون متعددی در جنگ سایبری وجود دارد که در دو بخش نرم افزار و سخت افزار قلبل اجرا هستند. هر کدام از این بخش ها بیانگر نوع نگاه خاصی به فضا و جنگ سایبری می باشد. در این

۱- white hat hackers
۲- Black hat hackers
۳- Gary hat hackers
۴- Pink hat hackers
۵- Red hat hackers

رویکرد دایره اثرگذاری و کارکرد نرم افزار و و سخت افزار جنگ های سایبری متفاوت است که در زیر به آن اشاره می‌شود [2].

الف– نرم افزار

- **ویروس‌ها–** نرم افزارهایی که پس از ورود به رایانه هدف نظیر ویروس‌های واقعی تکثیر و سبب سردرگمی نرم‌افزاری و یا انتقال به محیط شبکه کل سامانه را مختل می‌نمایند.
- **اسب تروا**– در دنیای دیجیتال یک بد افزار ضد امنیتی است که در ظاهری خوشایند مخفی و هنگام دریافت و باز نمودن یک فایل تصاویر و یا موسیقی دلخواه یک برنامه خطرناک در سیستم رها شده که می‌تواند کل دیسک را پاک و یا شماره کارت اعتباری و گذرواژه آن را به یک مقصد ناشناس ارسال نماید.
- **کرم**– برنامه‌هایی که خود را مکرراً تکثیر کرده و فضای حافظه را اشباع نموده و قادرند با تأخیر فعال شده و خود را در سراسر فضای شبکه تکثیر و سبب کند شدن سیستم گردند.
- **شنود**– برنامه‌ای که کلیه مکالمات و تبادلات مالی را شنود و از این راه نام‌ها، شناسه‌ها و گذرواژه‌ها را به دست می‌آورد.
- **برنامه های رمز شکن**– با استفاده از روش آزمون و خطای خودکار به کد و رمز سیستم‌ها دست پیدا کرده و نوع پیچیده توان بالقوه از کارانداختن سامانه حفاظتی سیستم‌های مورد حمله را دارد.
- **برنامه‌های برچسب**– یک برچسب شناسایی را در یک رایانه (درایور راه انداز آن) نصب و آن‌را برای نفوذ سایبری در آینده نشان گذاری می‌کنند.
- **بمب منطقی**–قطعه کدهای مخرب جاسازی شده‌ای که با ایجاد صدا در زمان معین و یا هنگام انجام عمل خاصی منفجر شده وپس از رهایی در محیط سیستم اثرات نامطلوب نظیر تخریب BIOS از خود به جای می‌گذارند [3].

ب– سخت افزار

- **میکروب**– باکتری های زنده ای که بر روی مواد خاصی از قطعات سخت افزاری سیستم ها نظیر سیلیکون و پلاستیک رشد کرده و تکامل می یابند و اگر وارد تجهیزات

الکترونیکی شـــوند مدارهای الکترونیکی و مواد عایق را خورده و ســـیســـتم را غیرقابل استفاده می نمایند.

- **نانو ماشـــین یا مورچه آتشـــین**- روبات‌های بســـیار ریزی که با انرژی خورشـــیدی کار می‌کنند و دارای حواس بینایی، بویایی، شـــنوایی و توان حرکت و انفجار بنا به دســـتور را دارا و قادرند از منافذ دســـتگاه‌های الکترونیکی وارد شـــده و مدارات الکترونیکی آن را تخریب نمایند.
- **اخلال تراشـــه‌ای**- تراشـــه‌های پیشـــرفته محتوی میلیون‌ها مدار الکترونیکی مجتمع که شـــرکت‌های ســـازنده قادرند به راحتی آن‌ها را برای بروز نقص و یا حتی انفجار در زمان معین یا پس از دریافت یک سیگنال با فرکانس خاص برنامه ریزی نمایند.
- **در نفوذ یا در پشتی** – مکانیسمی که در یک سیستم توسط سازنده آن تعبیه شده و راه عبوری به سیستم مورد نظر و عبور از گره‌های امنیتی عادی برای وی محسوب می‌شود.
- **بمب پالس الکترومغناطیسی**- نیروهای ویژه پس از نفوذ به مناطق عقب دشمن می‌توانند در نزدیکی تجهیزات آســـیب‌پذیر اقدام به تولید انفجار پالس الکترومغناطیســـی نمایند که سیستم های رایانه‌ای و ارتباطی را در شعاع عمل خود مختل نماید.
- **پارازیت دهنده‌ها** – ابزارهایی که در مراکز C4I، ســـامانه‌های پدافند هوایی، رادارها و سایر سلاح‌هایی که توسط رایانه کنترل می‌شوند.
- **فرکانس رادیوی پر انرژی** – توســـط فرســـتنده‌های رادیویی بر روی اهداف الکترونیکی ارسال و موجب اختلال در عملکرد آن می‌شوند.
- **دســـتگاه های الکترومغناطیس ـنلپلیدار**–پالس‌هایی تولید می‌کنند که دارای طول موج بسیار کوچکی بوده و می‌توانند برروی طیف وسیعی از ابزارهای الکترونیکی تاثیری شبیه صاعقه را ایجاد نمایند.

مفهوم جنگ ســایبری به دنبال ظهور فناوری‌های عصــر اطلاعات نظیر ماهواره، پســت الکترونیک، اینترنت، رایانه و ســـایر ریز تراشـــه‌ها و تبدیل جهان به یک دهکده مطرح گردیده اســـت. جنگ ســایبری هر ســه ضــلع مثلث دولت، ملت و نیروهای مســلح را شــامل می‌شــود و یکی از بارزترین تهدیدات ناهمطراز می‌باشـد. حملات سـایبری در راسـتای عملیات روانی، تروریسـم و خرابکاری قلمداد می‌شـود و به دلیل ارزانی ابزار فناوری اطلاعات در مقایسـه با سـایر فناوری‌های حوزه دفاع،

احتمال بهره‌برداری از جنگ سایبری در جنگ‌ها بسیار افزایش یافته است [4]. چنین حملاتی را تروریست‌ها برای گسترش وحشت، خلافکاران برای کسب درآمدهای نامشروع و یا دولت- ملت خاص برای رویارویی با دشمن به کار می‌گیرند. این جنگ نه تنها وب سایت‌های بخش‌های دولتی و خصوصی دشمن را مورد حمله قرار می‌دهد، بلکه هدف‌های با ارزش‌تر نظیر شبکه‌های کنترل تاسیسات و تجهیزات نظامی را نیز مدنظر دارد. برخی از مصادیق جنگ سایبری عبارتند از:

- انفجار و یا نقص در سیستم تسلیحات نظامی به دلیل خرابی رایانه‌ها.
- قطع کامل سیستم‌های تلفن و منابع تغذیه الکتریکی.
- استفاده از اینترنت (سایت‌های خبری عمده) برای انتشار اخبار دروغین یا از کار انداختن منابع خبری اینترنتی.
- ایجاد محرومیت از امکانات مخابراتی و ارتباطی.
- مختل نمودن سیستم کنترل ترافیک و حمل و نقل هوایی و ریلی.

سامانه‌های نظامی که به نوعی به رایانه‌ها متکی هستند در برابر جنگ سایبر آسیب‌پذیرند که نمونه هایی از آن عبارتند از: سامانه‌های فرماندهی و کنترل مکانیزه (C4ISR)- سامانه های مخابراتی و ارتباطی- سامانه های مراقبت و هشدار دهنده – سامانه‌های جنگ الکترونیک- دستگاه‌های رمز کننده و رمز گشا - شبکه‌های رایانه‌ای نظامی - سیستم‌های سلاح (سامانه‌های سلاح مدرن در توپخانه، زرهی، پدافند هوایی، پیاده و هوانیروز که برای تعیین موقعیت دشمن و اهداف، تعیین بردیا فاصله، رهگیری، آتش و سایر اعمال به رایانه متکی باشند اهداف خوبی را برای جنگ سایبری تشکیل می‌دهند). تعدادی از این موارد عبارتند از: کشف راداری، کنترل و هدایت موشک‌ها ،کنترل آتش، شناسایی دوست از دشمن و اطلاعات حاصله از سیستم موقعیت یاب جهانی(GPS).

مبانی نظری

بیان مسئله

بی گمان امنیت از مهم‌ترین دغدغه‌های بشر است. امنیت جان و امنیت غذایی و امنیت شخصی تا امنیت جمعی را می‌توان به عنوان مهم‌ترین انگیزه بشر و هدف از حرکت‌ها و کنش‌ها برشمرد. اگر دغدغه آرامش روحی و روانی برای هر فردی، دغدغه و هدف اصلی است، آرامش و امنیت جمعی نمی‌تواند از این دایره بیرون باشد و لذا امنیت و آرامش به شکل لایه‌های در هم تنیده خودنمایی

می‌کند. بنابراین تلاش انسان دست یابی به همه انواع و اقسام آرامش و امنیت و حفظ و نگه داشت آن اســـت. ویکی از مواردی که تامین امنیت را دریک جامعه به خطر می‌لندازد. وجود تهدیدات امنیتی درآن جامعه می‌باشد. به هرمیزان که تهدیدها افزایش یابد، ضریب امنیت ملی کاهش خواهد یافت. تهدیدات امنیتی سبب تجمیع وهمبستگی بین سازمان‌های امنیتی از جمله سپاه پاسداران و ارتش جمهوری اسلامی ایران شد.

بازیگران منطقه‌ای عموماً تمایلی به تغییر موازنه قدرت در حوزه نفوذ جغرافیایی خود ندارند. بنابراین هرگونه تحول منطقه‌ای، زمینه شـــکل گیری اقدامات مقابله جویانه بازیگران منطقه‌ای را فراهم می‌سازد. چنین شکل و سطحی از تهدیدها را می‌توان به عنوان دومین لایه از تهدیدهای امنیت ملی جمهوری اسلامی ایران دانست. زمانی‌که انقلاب ایران به پیروزی رسید، طیفی گسترده از کشـــورهای منطقه احســـاس تهدید کردند و درصـــدد برآمدند محدودیت‌هایی راهبردی علیه جمهوری اسلامی ایران به وجود آورند. در این شرایط، جلوه‌هایی از صدور انقلاب نیز در دستور کار مقامات سیاسی و اجرایی ایران قرار داشت. موضوع صدور انقلاب که بخشی از واقعیت ایدئولوژی یکی و ساختاری انقلاب ایران محسوب می‌شد، موجب ظهور واکنش‌های امنیتی و اقدامات تهدیدآمیز علیه ساختار سیاسی و فرآیند اجرایی ایران شد .[5]

هر کشوری که از توان برنامه‌ریزی و سازماندهی قابلیت‌های امنیتی بیشتری برخوردار باشد، قادر خواهد بود سطح متنوع‌تری از تهدیدهای امنیتی را سازماندهی کند. در چنین فرآیندی، قدرت‌های بزرگ قابلیت بیشتری برای سازماندهی چنین تهدیدهایی دارند، در حالی که بازیگران داخلی و منطق‌های کنش سیاسی خود را درروند تهدیدسازی به عنوان رفتار به انجام می‌رساند [6].

تهدیدهای کم شدت عمدتاً ماهیت فرهنگی، اجتماعی و سیاسی دارند. اینگونه تهدیدها دارای آثار و پیامدهایی طولانی مدت‌اند. کشورهایی مبادرت به سازماندهی تهدیدهای کم شدت می‌کنند که از برنامه‌ریزی سیستماتیک در سازماندهی تهدیدها برخوردارند. به عبارت دیگر، تهدیدهای کم شدت دارای آثار وضعی هستند و نتایج امنیتی خود را در طولانی مدت منعکس می‌سازند .این تهدیدها را می‌توان در زمره شاخص‌های تهدید نرم و جنگ نرم مورد توجه قرار داد که در کوتاه مدت به بحران‌های امنیتی پرشدت منجر نمی شوند.

از آنجا که ایران در محیط ژئوپولیتیکی ویژه‌ای در حوزه خاورمیانه، خلیج فارس و آسیای جنوب غربی قرار دارد، طبیعی است تهدیدها ماهیت متنوع و سازمان یافته‌تری پیدا کنند. زمانی‌که کشورها

در شـرایط ارتقای قدرت ملی خود قرار می‌گیرند، طبیعی اسـت جلوه‌هایی از همکاری گرایی و مشـارکت راهبردی بازیگران تهدیدکننده نیز به وجود آید .به عبارت دیگر، تهدیدها را می‌توان واکنشـی به شـاخص‌های قدرت و رفتار راهبردی بازیگران دانسـت. این فرآیند در دوران پس از پیروزی انقلاب اسـلامی ایران از گستره و ابعاد متنوع‌تری برخوردار شـد. تهدیدهای پرشـدت علیه امنیت ملی جمهوری اسـلامی ایران را می‌توان در ارتباط با سـازماندهی جنگ تحمیلی علیه ایران و اقدامات نظامی مسـتقیم نیروهای فرماندهی مرکزی آمریکا علیه اهداف اقتصـادی و راهبردی ایران درسال۱۹۸۸مورد توجه قرارداد [7].

تهدیدهای منطقه‌ای در شـرایطی انجام گرفت که تضـادهای فرهنگی و تاریخی بنیادین در نگرش کشـورهای خاورمیانه به سـنت‌های سـیاسـی و ایدئولوژیک ایران وجود داشـت. انقلاب ایران چنین ادراکی را تشـدید کرد. از سـوی دیگر، کشـورهای عرب خاورمیانه معتقد بودند هر گونه تعلل و تأخیر در انجام اقدامات مقابله جویانه در برابر انقلاب ایران، مخاطرات امنیتی برای آن‌ها ایجاد خواهد کرد. بنابراین،کشورهای محافظه کار منطقه درصدد برآمدند جلوه‌هایی از تولید قدرت برای مقابله با ایران را سازماندهی کنند که به منزله تهدید منطق‌های در برابر موجودیت سیاسی و رسالت گرایی راهبردی ایران بود.

تهدیدهای بین المللی شـــاخص‌های متنوعی دارند. از جمله این اقدامات می‌توان به تهدیدهای مستقیم و تهدیدهای غیرمستقیم اشاره کرد. قدرت‌های بزرگ ترجیح می‌دادند اقدامات خود را در قالب تهدیدهای غیرمسـتقیم سـازماندهی کنند، زیرا هزینه امنیتی کمتری داشـت. جلوه‌هایی از حمایت مالی برای گروه‌های ضـدساختاری، هم چنین حمایت راهبردی از عراق برای جنگ علیه ایران را می‌توان در زمره چنین اقداماتی دانسـت. اگر نظام سـیاسـی فاقد مشـروعیت اجتماعی و ساختاری بود، طبعاً با تهدیدهای متنوع امنیتی روبه رو می شد. مقابله با این تهدیدها از طریق بسیج نیروهای اجتماعی و مقابله مؤثر با تهدیدها انجام گرفت. جهت‌گیری سیاسی بسیاری از کشورهای خاورمیانه و خلیج فارس ماهیت محافظه کارانه داشته است که نشان می‌دهد. محافظه کاری بخشی از واقعیت سـیاسـی و راهبردی کشـورهای منطقه محسـوب می‌شـود .چنین نشـانه‌ها و فرآیندی، تضادهای امنیتی با ایران را باز تولید می‌کند [8].

در چنین وضـعی، نه تنها نهادهای سـیاسـی و امنیتی مؤثری برای کنترل بحران و تهدیدها وجود نداشـت، بلکه گفتمان امنیتی ایران نیز شـکل نگرفته بود. علاوه بر مؤلفه‌های یادشـده می‌توان

نشانه‌های قابل توجهی از انتظارات فزاینده گروه‌های سیاسی و اجتماعی را مورد ملاحظه قرار داد که در دوران پس از پیروزی انقلاب اسلامی شکل گرفت و به صورت مرحله‌ای تصاعد یافت. این روند تا جنگ تحمیلی و رویارویی مسلحانه گروه‌های سیاسی معارض تداوم پیدا کرد. زمانی‌که تهدیدهای امنیت ملی تشدید شد، زمینه برای تولید گفتمان امنیت ملی در قالب مؤلفه‌های هویت ایدئولوژ یکی در سازمان ارتش جمهوری اسلامی ایران به وجود آمد. تهدیدهای امنیت ملی در شرایطی شکل می‌گیرد که ساخت‌های سیاسی و امنیتی کشورها در وضعیت عدم انسجام قرار داشته باشند. این وضعیت در ماه‌ای اولیه پس از پیروزی انقلاب اسلامی ایران به وجود آمد. سازماندهی نهادهای جدید سیاسی و انقلابی نیازمند زمان، برنامه ریزی و هماهنگی رفتار نخبگان سیاسی بود. طبعاً تحقق این مسئله در مراحل زمانی اولیه پس از پیروزی انقلاب اسلامی کاری دشوار بود. به همین دلیل، شاهد تهدیدهای ترکیبی علیه امنیت ملی جمهوری اسلامی ایران بودیم. یکی از این سازمان‌ها که از انسجام کافی برخوردار نبود ارتش جمهوری اسلامی ایران بود. که رژیم بعثی عراق از این فرصت استفاده نمود. و به ایران حمله کرد [9].

تهدیدهای امنیتی در هر کشوری تابعی از شرایط سیاسی، اجتماعی، اقتصادی، نظامی و فرهنگی است. که این گونه تهدیدات تاثیر مستقیمی بر ساختار و ماموریت ارتش دارد. با توجه به اینکه تامین امنیت از وظایف اصلی ارتش می‌باشد. برای جلوگیری از غافلگیری و آمادگی جهت مقابله با آنها بایستی تهدیدات را در آینده پیش بینی کرد. کشور جمهوری اسلامی ایران که در ماه‌های اولیه پس از پیروزی انقلاب در فرآیند تحولات سیاسی قرار داشت . به گونه‌ای اجتناب ناپذیر از گفتمان امنیتی در ارتش بود. در غیر این صورت، با جلوه‌هایی از ناکارآمدی، گسترش بحران و فرسایش قدرت در نیروهای مسلح از جمله ارتش روبه رو می‌شد.

یکی از چالش‌های ارتش جمهوری اسلامی ایران درسال‌های آینده به طور مستقیم بااستمرار جریان‌های تروریستی در منطقه مربوط خواهد بود. حوادث سال گذشته در منطقه غرب آسیا نشان از آن دارد.که مهم ترین و بیشترین ماموریت ارتش در خارج از کشور در خصوص تروریسم بوده و مهم‌ترین پیامدهای حاصل از رواج تروریسم نیز د رمنطقه غرب آسیا و پیرامون آن قابل مشاهده است. تحولات میدانی ارتش و سپاه در سوریه ورشد تحرکات نظامی گروه‌های تروریستی به عنوان مرکز ثقل حوادث تروریستی، معمای ایجاد امنیت در منطقه را همچنان درهاله‌ای از ابهام قرارداده است. حمایت برخی از کشورهای مرتجع و حامی غرب ازگروه‌های تروریستی به عنوان

مهم‌ترین عامل استمرار ناامنی در سوریه همچنان در راس حوادث منطقه قراردارد. حوادث عراق وعملکردگروه تروریستی-تکفیری داعش محوردیگرناامنی درهمسایگی ایران است.

همچنین به نظر می‌رسد یکی دیگر ازمهم‌ترین چالش‌های امنیتی ارتش جمهوری اسلامی ایران درسال‌های آینده ناشی از تشدید تنش‌های احتمالی ایران و آمریکا با قرارگرفتن ترامپ در راس قدرت آمریکا باشد. درسال جاری میلادی، استمرار حضور آمریکا در منطقه به بهانه‌ی ساخت امنیت براساس راهبرد سازه انگاری وتلاش برای بدست گرفتن نقش پلیس جهانی از طریق تقویت روابط با برخی از کشورهای منطقه ازجمله عربستان وهمچنین استمرار مذاکرات با برخی از کشورهای عربی و غیر عرب منطقه از جمله مصر و ترکیه همچنان ادامه خواهد داشت. به نظر می‌رسد طی ماه‌های آینده این موضوع به واسطه حضور جمهوری خواهان وترامپ در راس قدرت آمریکا پررنگ‌تر شود. این اقدام به طور مستقیم وغیر مستقیم منجر به تشدید ناامنی‌های موجود در منطقه شده و به نوعی تشویق برخی از کشورهای عربی به خرید سلاح و تجهیزات غربی را در پی خواهد داشت به هرحال این اقدام به لحاظ تقویت قدرت نظامی کشورهای منطقه باید در دستور کارمقامات و مسئولین ایران از جمله ارتش قرارگرفته و اقدامات لازم برای تقویت اندیشه‌ی دفاعی و امنیتی از طریق توجه به اختصاص بودجه لازم وکافی برای تقویت قدرت نظامی و ساختار نیروهای مسلح از جمله ارتش مد نظر قرار گیرد. تاکید مقام معظم فرماندهی کل قواخطاب به فرماندهان و مسئولین نیروهای مسلح مبنی براینکه، انتظار دارم نسبت به معماری و طراحی نیروهای مسلح درافق بلند مدت برمبنای اندیشه‌ی دفاعی و امنیت جمهوری اسلامی ایران اهتمام ورزید. حاکی از اهمیت تقویت نیروهای مسلح و ارتش بوده و شایسته‌ی توجه واقدامی جدی است.

تجزیه و تحلیل

سلطه علمی کشورهای بیگانه با استفاده از مقالات علمی

در حقیقت کشورهای صاحب تکنولوژی و صنعتی هرگاه برای تولید و ساخت دستگاه و یا ارتقا تکنولوژی خود به مشکل جدی برخورد می‌کنند آن مشکل را به ده‌ها مسئله ریز تقسیم کرده تا کشورهای دیگر به اصل موضوع پی نبرند و با ایجاد پایگاه‌های علمی در قالب مقالات ISI[1] اقدام به جمع آوری مقالات علمی از سایر کشورها می‌نمایند. سپس هر مقاله خلاصه برداری و داده‌های

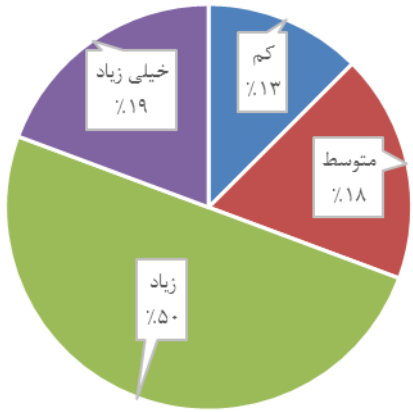
[1] ISI: Information Science Institute

آن استخراج و طبقه بندی شده و توسط محققان آن کشور استفاده شده و آن نیاز علمی رفع می‌شود که در نهایت منجر به تولید محصولات با فناوری بالا و پیچیده شده و دوباره با قیمت چندین برابر بالاتر در اختیار کشورهای غیر صنعتی جهان قرار می‌گیرد. در حقیقت کشورهای صنعتی با بهره‌برداری از نیروی جوان و تحصیل کرده کشورهای جهان سوم و همچنین منابع طبیعی این کشورها نوع جدیدی از استعمار نوین را ایجاد نموده است و یا با ایجاد تسهیلات مناسب از قبیل کار و شغل و درآمد نخبگان را از سایر کشورها به کشور خود جذب می‌نمایند. در حقیقت به دلیل ۱- عدم ارتباط دانشگاه‌ها با صنعت، ۲- عدم تبدیل مقالات علمی به کالا و تامین نیاز کشور، ۳- عدم حمایت مادی و معنوی از نخبگان که سبب مهاجرت گسترده به سایر کشورها می‌شود. واقعیتی که امروزه وجود دارد این است که کشورهایی که امروز صاحب علم و فناوری هستند، صاحبان قدرت در جهان به شمار می‌روند. طبیعی است ایران هم بخاطر اینکه از بحث‌های علمی و فناوری عقب نماند، در تلاش است تا به جایگاه مناسب و در خور خود در جهان دست یابد. از طرف دیگر، صاحبان استکبار در دنیا می‌خواهند این پیشرفت در انحصار خودشان باشد و مانع پیشرفت دیگر کشورها شوند. آن طور که از بیانات رهبر انقلاب اسلامی و نیز از سخنان کارشناسان سیاسی بر می‌آید می‌توان چنین نتیجه گرفت که دشمنان ایران اسلامی از دیرباز تاکنون در صدد جستجوی راه‌هایی برای وابسته کردن ایران به خود بوده و هستند. زمانی‌که ایران توانست در زمینه علم هسته‌ای پیشرفت چشمگیری حاصل کند، در کانون توجه مثلث شوم دشمن قرار گرفت. آنان روش‌های متعددی را برای جلوگیری از پیشرفت علم هسته‌ای ایران امتحان کردند، از بازدید از مراکز تأسیسات هسته‌ای تا امضای قطعنامه در شورای امنیت سازمان ملل... اما هیچ کدام از این راه‌ها پاسخگوی نیاز آنان نبود؛ لذا همان نقشه شوم همیشگی خویش یعنی ترور شخصیت و فرد را برگزیدند. خیال کردند که با حذف فیزیکی چند تن از دانشمندان هسته‌ای می‌توانند ضربه مهلکی به نظام بزنند [10]. این خیال، تصوری واهی بیش نبود چرا که به سرعت دانشمندانی جایگزین شده و با سرعت بیشتر به کار خود ادامه دادند. تهدیدها در شکل دیروز و مذاکره در شکل امروز هیچ کدام نخواهد توانست جلوی پیشرفت علمی ایران را بگیرد و جوانان با استعداد ایرانی به ندای رهبر خویش لبیک گفته و همواره در راه علم و ایمان آماده جهاد هستند. برای مقابله با این تهدیدها کشورهای جهان اسلام با ایجاد پایگاه داخلی به نام پایگاه علمی جهان اسلام ISC اقدام نموده تا بتوانند بدون وابستگی نیازهای خود را شناسایی و از طریق علمی و مقالات آنها را تامین

نمایند. در ادامه داده‌های استخراج شده از مصاحبه با صاحب نظران، گویای اهمیت زیاد این موضوع دارد که نیاز به توجه بیشتر مسئولان را نشان داده است.

جدول۱: پاسخ مصاحبه شوندگان در ارتباط با اهمیت سلطه علمی بیگانگان

عنوان سوال	پاسخ به سوالات			
اهمیت	کم	متوسط	زیاد	خیلی زیاد
سلطه علمی بیگانگان	11	16	44	17



شکل۱: درصد رای صاحب نظران بر میزان و اهمیت تهدید سلطه علمی کشورهای بیگانه

وابستگی نرم افزاری

کشور ما نیز که تازه گام در مسیر توسعه گذاشته همواره از دو بعد داخلی و خارجی در معرض تهدید امنیتی بوده و این تهدید کما کان ادامه دارد. منظور از تهدیدات نرم افزاری آن نوع تهدیداتی است که متاثر از عوامل چهار گانه سیاسی، اقتصادی، اجتماعی و فرهنگی بوده و با توجه به موقعیت داخلی امنیت یک کشور را باخطر مواجه به می‌کند. در مقابل تهدیدات نرم افزاری تهدیدات سخت افزاری قرار دارد. هجوم نرم افزارهای بیگانه به داخل کشور و دادن امکانات به شهروندان به صورت رایگان فرصت‌ها و خطرات فراوانی را پیش روی کشور ایجاد می‌کند، از آنجایی که اطلاعات مبادله شده در این نرم افزارها درون پایگاه داده ذخیره می شود بعدها می‌تواند زمینه جاسوسی‌های زیادی را ایجاد نماید. از جمله معضلات استفاده گسترده از این اپلیکیشن‌ها بدون فرهنگ‌سازی و آموزش نحوه استفاده را می‌توان به موارد زیر اشاره نمود.

الف: تهدیدات فرهنگی– اجتماعی در نرم افزارها:

۱- تهاجم فرهنگی: تهاجم فرهنگی را باید مجموعه اعمال آگاهلنه و با هدف دشـــمن برای تغییر آگاهی‌ها در گرایش‌ها تمایلات مردم از حوزه تفکرات دینی و اسلامی به حوزه جهان بینی مادی و الحادی دانسـت. نتیجه این تهاجم اختلال در روابط اسـتراتژیک مردم با نظام سـیاسـی و حکومت دینی اسـت. تهاجم فرهنگی زمینه افزایش توقعات مردم را در داخل فراهم خواهد کرد. بخشـی از افزایش توقعات مردم را باید در تهاجم فرهنگی برنامه‌ریزی شده و کنار زدن فرهنگ بومی و ترویج ارزش‌های ضد ملی و دینی مانند فرهنگ تجمل گرایی اشرافی‌گری چشم هم چشمی و....دانست بالطبع دولت نیز با معضـلات اقتصـادی متعددی دسـت به گریبان اسـت و قدرت بر آوردن همه توقعات مردم و یا توقعات همه مردم را ندارد. لذا روزبروز بر نارضـایتی مردم از دولت و حکومت به تبع عدم ارضای نیازها و توقعات متاثر از ارزش‌های تزریق شده به واسطه تهاجم فرهنگی افزوده خواهد شـد که خود یک مقوله ضـد امنیتی بوده و حکومت را با بحران‌های درونی مواجه خواهد کرد. امروزه تهاجم فرهنگی از طریق گسترش ابزارهای اطلاع رسانی و استفاده نادرست از آنها و عدم فرهنگ سـازی در باره چگونگی اسـتفاده از نقاط مثبت تکنولوژی روز صـورت می‌گیرد. در جهان کنونی بخش عمده‌ای از چالش‌های حکومت‌های جهان سـوم را حاکمیت ماهواره‌ها و اینترنت تشـکیل می‌دهند. اگر از حاکمیت بلامنازع این ابزارها جلوگیری شـود و تنها در قالب‌های غیر مخرب استفاده گردند. به نقض حقوق انسانی و نبود جریان آزاد اطلاعات متهم می شوند و در صـورت آزادگذاری مطلق و بدون هیچ محدویتی به دلیل فرهنگ سـازی نکردن در خانواده‌ها و محیط‌های آموزشـی و همچنین نبود فرهنگ صـحیح چگونگی اسـتفاده از ابزارهای اطلاع رسـانی خودبخود حکومت‌ها زمینه تغییرات فرهنگی جوامع جهان سـومی با حاکمیت ماهواره و اینترنت به خطر می‌افتد. لذا تنها راه حل ایجاد پاد زهر یعنی تقویت فرهنگ‌های ملی بومی و اسـلامی توام با محدودیت قانونی قایل شدن می‌باشد.

۲- ارتجاع: معنای مورد نظر ما از ارتجاع عبارتسـت از بازگشـت به ارزش‌های فرهنگی دوران قبل از انقلاب عالمان علم سیاست آخرین مرحله یک انقلاب را دوران تر میدور می‌دانند. در این دوران است که شعارهای واقعی و اصلی و اهداف حقیقی یک انقلاب فراموش شده و در مردم آرزو و یا به تعبیر دیگر شـوق پذیرش ارزش‌های دوران قبل از وقوع انقلاب در آنها پدید می‌آید. لذا خطرناکترین تهدید امنیتی کشـور را می‌توان دوره تر میدور به حسـاب آورد. علل بوجود آمدن

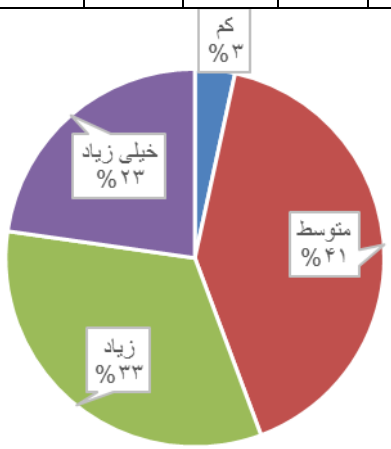
این دوره نیز ناتوانی و ناکامی حکومت گران از بر آوردن شعارهای انقلاب اهداف و آرمان‌های آن و کنار گذاردن مردم از صحنه و خنثی در نظر گرفتن فعالیت‌های مردم بر می‌گردد. انقلاب اسلامی حرکتی انقلابی در روحیات افکار اخلاق و اعتقاد بوده و از اینرو فرهنگ تجمل پرستی راحت طلبی فساد اخلاقی سیاسی و اداری تبعیض بی عدالتی رشوه خواری را از مظاهر رژیم شاهنشاهی می‌دانست. اما اکنون بعد از گذشت چهار دهه از انقلاب شاهد ظهور و رشد مجدد این ارزش‌ها و فرهنگ‌ها در دستگاه‌های نظام و در سطح جامعه هستیم که در صورت چاره نیاندیشی پایه‌های اقتدار سیاسی و امنیتی نظام را متزلزل خواهد کرد که بیشتر این نوع تفکر بخاطر عدم کنترل نرم افزارها و تزریقات از جارج از کشور بوده است.

ب: تهدیدات سیاسی این نرم افزارها:

تجدید نظر طلبی: تجدید نظر طلبی نه به معنای اصلاح عیوب بلکه به معنای تغییرات اساسی در ساختار حکومت و احیانا تغییر و انطباق آن با آموزه‌های لیبرالیسم می‌باشد. تجدید نظر طلب‌ها در کشور ساختار کنونی قانون اساسی کشور را مغایر با حقوق شهروندی می‌دانند. از اینرو خواهان تغییر قانون اساسی می‌باشند. تجدید نظر طلب‌ها در جریان‌ها و جناح‌های سیاسی در کشور را بر عهده دارند. بنابراین رویکرد جریان‌ها و جناح‌های سیاسی لیبرال‌منش به آموزه‌های مکاتب اومانیستی سیاسی غرب و رد نظریات دین درباره ایجاد حکومت مردمی و توسعه گرا از سوی این جریان‌ها را باید یک تهدید امنیتی به لحاظ سیاسی به حساب آورد. مهمترین مولفه‌های قدرت در جمهوری اسلامی ایران ایمان توده‌های مردم هدایت رهبر و ایدئولوژی انقلابی است. بنابراین نقاط آسیب پذیر به لحاظ داخلی نیز با حفظ این سه عنصر مورد تجربه و تحلیل قرار می‌گیرد. هر عاملی که باعث سستی در ایمان مردم بوده و موقعیت رهبری را تضعیف نماید و اید ئولوژی انقلابی مردم را که ملهم از مبانی دینی و تعلیمات تشیع می‌باشد را به زیر سوال برده یک تهدید امنیتی به حساب می‌آید و چون تجدید نظر طلب‌ها که درون احزاب چپ گرای کنونی لانه کرده‌اند به دنبال تضعیف هر سه عناصر فوق بوده‌اند یک تهدید امنیتی اند. که می‌توان از مصادیق این اقدامات خبیث آمیز را کانال‌های آمد نیوز و ... بر شمرد. حال به بررسی نظرات صاحب نظران درباره میزان اهمیت خطرات ناشی از عدم کنترل نرم افزارها و اپلیکیشن‌ها پرداخته شده است.

جدول۲: پاسخ مصاحبه شوندگان در ارتباط با اهمیت وابستگی نرم افزاری

پاسخ به سوالات (اهمیت)				عنوان سوال
خیلی زیاد	زیاد	متوسط	کم	اهمیت
۲۰	۲۹	۳۶	۳	وابستگی نرم افزاری



شکل۲: درصد رای صاحب نظران بر میزان و اهمیت تهدید وابستگی نرم افزاری

تهدیدات سایبری

بیش از دو دهه است که اینترنت نقش بسزایی در ارتباطات جهانی ایفا می‌کند و به طور روزافزونی با زندگی مردم جهان عجین شده است. نوآوری‌ها و هزینه کم در این زمینه باعث شده دسترسی، استفاده و عملکرد اینترنت، به میزان قابل توجهی افزایش یابد، به طوری که امروزه اینترنت در سراسر دنیا در حدود ۲ میلیارد کاربر دارد. اینترنت شبکه وسیع جهانی را به وجود آورده که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری داشته است. با وجود این، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس‌بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی

برخوردارند و بازیگران آن را دولت- ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید. انواع تهدیدهای سایبری بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهم‌ترین آنها عبارتند از :جنگ سایبری، تروریسم سایبری، جرایم سایبری، جاسوسی سایبری و آشفتگی سایبری.

جنگ سایبری[1]

اگر با نظر کلازویتز موافق باشیم که جنگ عمل صرفاً سیاسی نیست، بلکه ابزار سیاسی برای رسیدن به اهداف سیاسی است، می‌توانیم بگوییم که جنگ در فضای مجازی توسط بازیگرانی صورت می‌گیرد که به دنبال استفاده از این فضا برای رسیدن به اهداف سیاسی خود هستند. به منظور درک اینکه آیا عمل خصمانه در فضای مجازی جنگ قلمداد میشود یا نه، لازم است قصد بازیگر را درک کنیم. به عنوان مثال، اگر هدف از یک حمله اینترنتی سود مالی یا شخصی از طریق روش‌های مجرمانه مانند سرقت، تقلب و اخاذی باشد، باید با آن به عنوان عمل مجرمانه برخورد شود، اما اگر هدف مهاجم با جاه‌طلبی‌های به مراتب بزرگ‌تر همچون واردکردن آسیب جدی به دولت یا شهروندان آن همچون تخریب، تضعیف و غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی باشد، چنین رفتاری در واقع چیزی نزدیک به اقدام جنگی در مفهوم سنتی است [11]. در سال 2007 استونی به عنوان کشور کوچک مدرن در مقیاس بزرگ مورد حمله‌های اینترنتی قرار گرفت. فنآوری بالای این کشور زمینه‌های مناسب برای حمله‌های اینترنتی با انگیزه‌های استدلال می‌کند، جنگ ۱ سیاسی بود [12]. همان‌طور که ریچارد کلارک سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به طور کامل درک کنیم .در عین حال، روشن است که در دنیای امروز، میدان جنگ حوزه خود را به فضای مجازی گسترش داده و باید آن را به عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین، هوا، دریا و فضا در نظر گرفت.

[1] -Cyber War

حمله سایبری[1]

حمله سایبری چیزی متفاوت از جنگ سایبری است. حمله سایبری اختلال در صحت یا درستی داده‌هاست که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، صورت می‌گیرد [13] حمله‌های سایبری شامل چهار حوزه می‌شود: ۱ –از دست دادن تمامیت، ۲ –از دست دادن قابلیت، ۳ –از دست دادن اطلاعات محرمانه و ۴ –تخریب فیزیکی [14] آب، برق، بانکداری و حمل‌ونقل هوایی، تنها چند نمونه از خدماتی است که توسط زیرساخت‌های اطلاعات و ارتباطات در حال اجراست. این زیرساخت‌ها به طور فزایندهای به یکدیگر وابسته هستند و هر حمله اینترنتی می‌تواند همانند بازی دومینو در آنها اختلال ایجاد کند. اختلال در یک سیستم مساوی با اختلال در دیگر سیستم‌هاست و ادامه این روند از تأثیرات بالقوه اینترنتی حمل است[15] .

تروریسم سایبری[2]

آژانس مدیریت فوق العاده فدرال، تروریسم سایبری را اینگونه تعریف می‌کند: تهدید و حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن، زمانی‌که برای ترساندن یا مجبورکردن حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد .تروریست‌ها با از دست دادن پایگاه‌های فیزیکی کلیدی (مانند افغانستان)، به عامل کلیدی برای اقدام در فضای سایبری تبدیل شده‌اند. این اقدام‌های می‌تواند شامل افزایش منابع برای حمایت از عملیات‌های خود، برنامه‌ریزی عملیات (استفاده از ابزارهای در دسترس همانند earth Google)، فرماندهی و کنترل عملیات، انجام عملیات‌های نفوذی و آموزش به هواداران خود (استقرار وسایل انفجاری) باشد [16].

جرایم سایبری[3]

جرایم اینترنتی می‌تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار تجاری و غیره باشد. این جرایم، همچنین شامل حمله عمدی به رایانه‌ها به منظور مختل‌کردن آن‌ها و یا کپی از اطلاعات طبقه بندی شده می‌شود [17]. تحلیلگران هزینه جرایم اینترنتی را برای صنعت جهانی بیش از هزار میلیارد دلار در موارد نقض مالکیت فکری و از دست دادن اطلاعات تخمین زده‌اند.

---

[1]-Cyber Attacks
[2] - Cyber Terrorism
[3]- Cyber Crime

برای مثال، شخصی در سال ۲۰۰۹ ،چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه جنگنده‌های مشترک ۳۰۰ میلیارد دلاری پنتاگون را به سرقت برد. علاوه بر این، بیشتر مجرمان اینترنتی از مجازات فرار کرده‌اند. بدیهی است این فعالیت پرسود و اغلب بدون مجازات، در واقع تهدیدی برای امنیت ملی است [18].

جاسوسی سایبری[1]

جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع آوری کند. برخلاف جرایم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی [19].

آشفتگی سایبری[2]

آشفتگی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرارداده و یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می‌کنند که غیرقانونی هستند .گروه‌های هکری آنارشیستی و نیهیلیست‌ها از آشفتگی سایبری استفاده می‌کنند. به عنوان مثال، ، مدیر سایت جنجالی ۳ گروهی تحت عنوان «ناشناخته‌ها» در واکنش به دستگیری جولیان آسانژ ویکیلیکس، حمله‌های سایبری گستردهای انجام دادند. برخلاف جرایم سایبری و جاسوسی سایبری که هدفشان دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف‌های خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده و یا تغییر یابد و یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود، اما قصد و نیت اصلی آشفتگی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تا کنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند (۱۸). Sharp and Lord : تهدیدهای سایبری از ماهیتی متنوع، گسترده و منحصر به فرد برخوردارند. متنوع از آن رو که این تهدیدها تمام حوزه‌های زندگی بشر را تحت

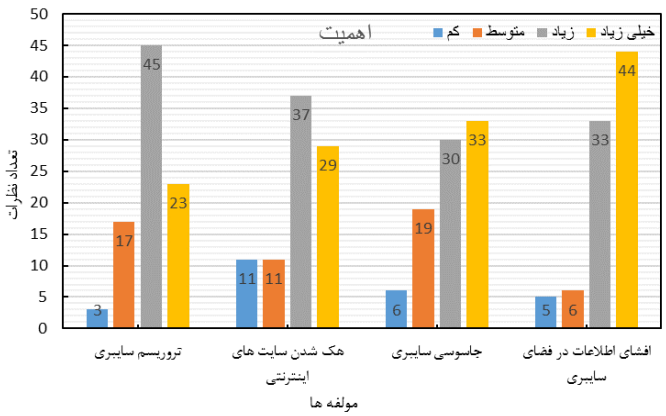
---

[1] - Cyber Espionage
[2] - Cyber Agitation

عنوان سوال	پاسخ به سوالات (اهمیت)			
اهمیت	کم	متوسط	زیاد	خیلی زیاد
تروریسم سایبری	۳	۱۷	۴۵	۲۳
هک شدن سایت‌های اینترنتی	۱۱	۱۱	۳۷	۲۹
جاسوسی سایبری	۶	۱۹	۳۰	۳۳
افشای اطلاعات در فضای سایبری	۵	۶	۳۳	۴۴

جدول۳: پاسخ مصاحبه شوندگان در ارتباط با اهمیت تهدیدات سایبری

تأثیر قرار داده‌اند و در نتیجه عدم امنیت در فضای سایبری بسیار بالاست. گستردگی نیز از آن رو که نه تنها بازیگران دولتی، بلکه شرکتهای خصوصی، گروه‌ها و افراد را نیز درگیر خود کرده است و منحصر به فرد بودن نیز بدین علت است که ماهیت این تهدیدها متمایز از تهدیدهای سنتی و رایج گذشته است که البته، این ویژگی بیشتر دولت‌ها و درک آن‌ها از تهدید را تحت تأثیر قرار داده است.



شکل۳: مقایسه میزان اهمیت تهدیدات سایبری بر اساس پاسخ صاحب نظران

تأثیر تهدیدهای سایبری بر امنیت ملی

بسیاری از کارشناسان و تحلیلگران حوزه امنیت، بر این باورند که پایان یافتن دوران جنگ سرد نه تنها منجر به امن‌ترشدن جهان نشده است، بلکه بـه وجـود آمـدن چـالش‌هـای امنیتـی غیرنظامی جدیدی همچون تخریب محیط زیسـت، رفاه اقتصـادی، سـازمان‌های جنایی بین المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدیتری نسـبت بـه گذشـته مواجـه ساخته است. تحلیلگران بر این باورند که اهمیت این مسائل "جدید" نـه تنهـا بازاندیشـی در تهدیدهای امنیتی، بلکه تجدید نظر درباره خود مفهوم امنیت را ضـروری می‌سـازد .در عین حال، انتقادی که بر ادبیات موجود امنیت وارد است این است که اغلب این متـون بـه تهدیدهای سایبری به عنوان یکی از همین چالش‌های امنیتی جدید که در ایـن زمینـه بسـیار هـم پراهمیت به نظر می‌رسد، توجه اندکی داشـته‌اند. همانطور که در بخش‌های پیشین اشـاره شـد، آنچه در مورد این تهدیدهای جدید قابل توجه اسـت، این اسـت که ویروس‌ها، کرم‌ها، جرم‌ها، هکرها و حملات اینترنتی، امروزه واقعیت مسـلم و روزمره هسـتند. حملات مخرب مهم با تأثیرات گسـترده، تهدیدهای سـایبری را به عنوان یکی از بدترین تهدیدهای منافع ملی به تصـویر کشـیده اسـت تـا جایی که ایالات متحده آمریکا اعلام کرده اسـت که این حملات را به عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد. از طرف دیگر، بحث و گفتگـو دربـاره ایـن تهدیـدات متـأثر از انقلاب مداوم اطلاعات و رسـوخ آن به تمام جنبه‌های زندگی بشـر امروز اسـت. بنابراین، در بخش پیش رو، ابتدا به انقلاب اطلاعات و تأثیر شگرفی که بر روی قدرت و منـابع آن خواهـد داشـت پرداخته و سپس از این رهگذر، تهدیدهای سایبری وابسته به آن و تأثیری که می‌تواند بـر امنیـت ملی داشته باشد، مورد بررسی قرار خواهد گرفت. در ادامه می‌توان گفت: فضای سایبری و فناوری‌های وابسته به آن، یکی از مهم‌ترین منابع قـدرت در هـزاره سـوم هستند. ویژگی‌های فضـای سـایبری همچـون قیمـت پـایین ورود، گمنـامی، آسـیب پذیر

و نامتقارن بودن، پدیده انتشـار قدرت را به وجود آورده اسـت، بدین معنی که اگر تاکنون دولت‌ها بازی قدرت را تنها میان خود تقسیم کرده بودند، از این پس بایـد آن را بـا بـازیگران دیگـری همچون شرکت‌های خصوصی، گروه‌های سـازمان یافتـه تروریسـتی و جنـایی و افـراد تقسـیم نمایند، اگر چه هنوز این دولت‌ها هستند که در این عرصه نقش مهمـی را بـازی مـی‌کننـد. بـه طبع، این پدیده امنیت ملی دولت‌ها را از تأثیرگذاری خود بی نصـیب نخواهد گذاشـت. این

تأثیرگذاری را از چند جهت می‌توان مورد ارزیابی قرار داد. نخست، مفهوم امنیت است .دیگر نمی‌توان امنیت ملی را همانند گذشته در ارتباط با مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد، بلکه امروزه، خطر افت کیفیت زندگی شهروندان نیز نوعی تهدید برای امنیت ملی محسوب می‌شود. دوم، از میان رفتن بعد جغرافیایی در تهدیدهای سایبری است. در گذشته، تهدیدهای نظامی از محل جغرافیایی خاصی برخوردار بودند. در نتیجه، مقابله با آن دست کم از جهت شناسایی کار چندان دشواری نبود. سوم، گستردگی آسیب پذیری‌های ناشی از تهدیدهای سایبری است. این تهدیدها پراکنده، چندبعدی و چندسویه‌اند و چون در ارتباط با شبکه‌های ارتباطی و زیرساخت‌های حساس می‌باشند، سطح آسیب رسانی آن‌ها بسیار بالاست. چهارم، این تهدیدها را صرفاً با شیوه‌های سنتی همانند به کارگیری ارتش و نیروی پلیسی نمی‌توان مهار کرد و برای مقابله با آن‌ها تلاش دولت‌ها به تنهایی کافی نیست و همکاری مؤثر و دوجانبه دولت‌ها و بخش خصوصی را که دارای منافع مشترکی در برخورد با اینگونه تهدیدها هستند، می‌طلبد. پنجم، همانگونه که از نکته قبلی بر میآید، تهدیدهای سایبری صرفاً متوجه دولت‌ها نیست، بلکه افراد و شرکت‌ها نیز از آسیبهای این تهدیدها بی‌نصیب نخواهند بود. ششم، چون امنیت در عصر اطلاعات صرفاً دولت محور نیست، بنابراین رویکردهای مختلف نظری در روابط بین الملل که به طور عمده بر مبنای دولت محوری به ساختاربندی نظریات خود پرداخته‌اند، یا به راحتی از کنار این تهدیدها گذشته‌اند و یا در تحلیل‌های خود با سردرگمی مواجه شده‌اند. در پایان، ذکر این نکته ضروری است که مجموعه عوامل بالا سبب خواهد شد دولت‌ها و محافل دانشگاهی دیر یا زود در برداشت‌های خود نسبت به منافع، پایگاه‌های قدرت و امنیتشان تجدید نظر کنند. لذا پاره‌ای از اقدامات که می‌تواند تا حدودی آسیب پذیری نیروهای مسلح و ارتش جمهوری اسلامی ایران را در جنگ آینده در برابر حملات سایبری کشورهای متخاصم کاهش دهد به شرح زیر پیشنهاد می‌گردد:

الف- آگاه سازی سایبری: همگام با پیشرفت فناوری اطلاعاتی آسیب پذیری‌ها نیز افزایش یافته و اهمیت ارتقای آموزش و دانش سایبری همه کارکنان آجا بیش از پیش گردیده است. برای این مهم لازم است تا سرفصل آموزش‌های مرتبط با موضوع در مدارس و دانشگاه‌های آجا در همه مقاطع گنجانیده شود .هم چنین در بخش‌های تحقیق و توسعه همه سازمان‌ها و یگان‌های آجا اهمیت موضوع تبیین و تحقیقات مرتبط با مقولات جنگ‌های نوین دارای اولویت گردند.

ب- **ایجاد امنیت در شبکه**: اقدامات تامینی لازم برای محافظت از سیستم‌های ارتباط و مخابرات آجا به عمل آمده و روش‌های اثر بخش برای جلوگیری از ورود عوامل غیر مجاز، کشف حملات سایبری، ریشه کن کردن ویروس‌ها، کرم‌ها و سایر عوامل مزاحم به سیستم‌ها به مورد اجرا گذارده شود. طرح تامین لازم برای مقابله با حملات سایبری که در برگیرنده خط مشی‌های لازم برای مقابله با شرایط قابل پیش بینی و غیر قابل پیش بینی را داشته باشد، باید مبتنی بر طرح‌های امنیت ملی تدوین گردد. تجهیزات موجود الکترونیکی و مخابراتی باید توسط متخصصین خبره و متعهد داخلی به دقت بازرسی گردیده تا از عاری بودن آنها از آلودگی‌های پیش گفته اطمینان حاصل گردد.

ج- **خودکفایی تجهیزاتی**: برای دستیابی به امنیت واقعی چاره‌ای جز اجتناب از واردات تجهیزات خارجی و اتکا به تولیدات خانگی رایانه، وسایل مخابراتی و سیستم‌های تسلیحاتی و نظایر آن وجود ندارد. علاوه برآن نیاز به سرمایه گذاری بومی در بخش نرم افزار نیز بسیار ضروری به نظر می‌رسد.

د- **اتخاذ مشی فعال جنگ اطلاعاتی سایبری:** نقاط ضعف سیستم‌های مخابراتی و الکترونیکی دشمن را باید شناسایی نموده و در حوزه جنگ سایبری مشی فعال را اتخاذ و تجربه و تبحر کافی را در زمینه به کار گیری ویروس، میکروب، کدهای رمزشکن، نفوذگری، ارسال پارازیت و غیره کسب نمود

نتیجه گیری با گسترش انقلاب های تکنولوژیک و اطلاعاتی و پیچیده تر شدن مناسبات اقتصادی و تولیدی در عصر جهانی شدن، ازیک سو مفهوم قلمروزدایی مطرح شده است و از سوی دیگر تغییر ماهیت تهدیدهای امنیت و مفهوم مرز و حراست از آن را به مسئله ای حیاتی بدل ساخته است. بنابراین، ویژگی جهانی و بدون مرز بودن این فضا با توسل به فناوری اطلاعات، امنیت ملی را با چالشی جدی مواجه کرده است. بنابراین، به عنوان یک نتیجه گیری کلی می‌توان گفت هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده تا بازیگران اعم از دولت‌ها، گروه‌های سازمان یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و ... را به وجود آورند .جمهوری اسلامی ایران نیز به دلیل آنکه محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی شماری را دربردارد

همانند هر کشور دیگری نیازمند استراتژی جامعی برای مقابله با این مسئله در جهت تضمین امنیت و دستیابی به منافع حیاتی خود از جمله انرژی هسته‌ای می‌باشد و لزوم برنامه ریزی و مقابله با این مسئله به عنوان یکی از مهم‌ترین تهدیدها و آسیب ها با توجه به اقدامات تخریبی علیه آن 14 و ...ناگزیر می‌نماید .لذا با اتخاذ یک روش و برنامه ریزی مناسب می توان این روند را معکوس نمود و » استاکس نت « نظیر مهم‌ترین کار ویژه امنیتی یک نظام، یعنی تبدیل تهدیدها به فرصت‌ها را صورت داد.

و- آموزش خبرگان نفوذگر: در زمینه آموزش و تربیت خبرگان نفوذگر درسیستم های الکترونیکی و مخابراتی باید اقدامات جدی در مراکز آموزش فرهنگی آجا به عمل آید.

ه- هماهنگی اقدامات جنگ سایبری در بالاترین رده: اهمیت جنگ سایبری ایجاب می‌نماید که هماهنگی‌های لازم برای اتخاذ مشی لازم در سطح ملی و با مشاورت خبرگان نظامی صورت پذیرد .در حال حاضر فقدان چنین هماهنگی سبب از

هم گسیختگی و عدم ورود صحیح ارکان کشور در این عرصه گردیده است به نحوی که امکان ارزیابی واقعی جایگاه کشور و آجا در این عرصه و وضعیت دشمنان بالقوه آن وجود ندارد. در این رابطه تشکیل یک هسته سیاست گذاری در سطح ملی با حضور کلیه عناصر ذیربط در وزارت علوم، تحقیقات و فناوری و یا وزارت دفاع ضروری می باشد. در هر صورت آنچه که از اهمیت بالایی برخوردار است دستیابی به یک راهبرد ملی در زمینه جنگ سایبری است که تابعی از راهبرد دفاعی کشور می باشد.

ز- شناسایی و به کارگیری کلیه امکانات بالقوه سایبری در کشور: شرکت‌های پیشرو در تولید نرم افزار، دانشگاه‌های صنعتی معتبر، کارخانجات الکترونیکی پیشرفته، مراکز تحقیقاتی صنعتی و غیر صنعتی، جشنواره های علمی معتبر، همایش‌ها و نمایشگاه‌های تخصصی و نظایر آن بستر و زمینه‌های علمی و فنی مورد نیاز کشور را اداره و ارائه می‌نمایند که لازم است در راستای نیازمندی‌های آجا شناسایی و از آنان بهره برداری به عمل آید. ترکیبی از خبرگان و متخصصین فناوری اطلاعات در آجا و بخش‌های یاد شده می‌توانند زمینه لازم برای تشکیل یک نیروی واکنش سریع سایبری را فراهم آورده و در موقع لزوم در اسرع وقت نسبت به انجام عملیات آفندی و یا پدافندی اقدام نمایند.

ر-ایجاد ساختار سازمانی مناسب در آجا: به منظور ورود در عرصه جنگ سایبری و هماهنگی عملیاتی، ایجاد ساختارهای هماهنگ کننده ستادی و یگان‌های عملیاتی در همه سطوح آجا ضروری است.

نتیجه گیری

هیچ نشانه‌ای از کاهش سرعت رشد انقلاب اطلاعاتی مشهود نیست. جنگ سایبری یکی از قلمروهای مطرح در عرصه برخوردهای بین المللی در سال‌های آغازین هزاره سوم بوده و فرصت‌ها و تهدیدهای قابل توجهی را در عرصه امنیت ملی و دفاع مطرح نموده است. بی شک عدم توجه کافی به این زمینه، تهدیدها را بالفعل نموده و فرصت‌ها را خواهد سوخت. وابستگی فناورانه به کشورهای بیگانه بالاترین تهدید و تلاش در زمین خودکفایی سایبری بالاترین اولویت در راهبرد جنگ سایبری است. بنابراین تشکیل هسته‌های سیاست گذاری در سطح ملی و ساختارهای واکنش سریع در حوزه دفاع ازاهم امور است. آن چه که امروز بسیار اهمیت دارد استفاده از زمان و تسریع در طرح ریزی جنگ سایبری در آجا می‌باشد. با توجه به تحلیل داده های استخراج شده از نظر سنجی‌ها و مصاحبات صورت گرفته توسط اساتید نظامی، مشخص شد بالاترین درجه و اهمیت تهدید افشای اطلاعات و تروریسمم سایبری بوده که نیاز به توجه بیشتر مسئولان زیربط دارد.

منابع

۱. ر. ز. مجتبی, " تدوین راهبردهای دفاع سایبری ارتش جمهوری اسلامی ایران," *فصلنامه مدیریت نظامی*, جلد ۵۹, p. 106, 1394.

۲. ب. ایرج, " مقاله تبیین نقش جنگ سایبری در جنگ های آینده," *فصلنامه علوم وفنون نظامی*, جلد ۲۸, p. 48, تابستان ۱۳۹۳.

۳. ر. ز. مجتبی, " تدوین راهبردهای دفاع سایبری ارتش جمهوری اسلامی ایران," *فصلنامه مدیریت نظامی*, جلد ۵۹, p. 109, پاییز ۱۳۹۴.

۴. ف. گراهام, قبله عالم: ژئوپلتیک ایران، ترجمه عباس مخبر, تهران, ۱۳۷۲ .

۵. ا. اصغر, کالبدشکافی تهدید, تهران: انتشارات دانشگاه عالی, ۱۳۸۷ .

۶. م. ابراهیم, نظام دوقطبی و جنگ ایران- عراق, تهران: انتشارات مرکز اسناد و تحقیقات دفاع مقدس, ۱۳۸۸ .

۷. بیانات مقام معظم رهبری در دیدار جمعی از نخبگان و برگزیدگان علمی, ۱۳ مهرماه ۱۳۹۰.

۸. ا. ت. پ. ب. ع. ابراهیم, " راهکارهای مقابله باتهدیدهای سایبری علیه جمهوری اسلامی ایران با تأکید بر نقش فناوری و منابع انسانی," *فصلنامه راهبرد دفاعی*, جلد ۵۰, p. 105, تابستان ۱۳۹۴.

انگلیسی

1. A. Ehteshami, "Iran's Revolution: Fewer Ploughshares, More Swords," *Army Quarterly and Defense Journal*, vol. 120, 1990.

2. R. Takeyh, Hidden Iran: Paradox and Power in the Islamic Republic, New York: Times Book, 2006.

3. P. Cornis, D. Livingstone, D. Clemente and C. Yorke, "Cyber Security: accept vulnerability World Foresight Forum is an initiative of Doctrine Command," A Chatham House Report, www.chathamhouse.org.uk, vol. 2, no. 1, 2011.

4. H. T. Klaar, "Cyber Security Threats and Responses: At Global, Nations State," www.Ceri-Scienes-po.org, 2011.

5. C. Rodriguez, "Cyber terrorism," Inter-American Defense College as a prerequisite for the Diploma approved, 2006.

6. U. Army, "Cyber Operations and Cyber Terrorism," U.S. Army Trainin, 2005.

7. Q. Islam, D. V. Teun and R. Marjolein, "Dealing with Cyber Security: accept vulnerability," World Foresight Forum is an initiative of, 2011.

8. S. Starr, "Towards an Evolving Theory of Cyber power," Center for Technology and National Security Policy, 2009.

9. D. Nagre and P. Warade, "Facts Behind The Myth," Cyber Terrorism Vulnerabilities and Policy Issues, 2008.

10. A. Peritz and M. Sechrist, "Protecting Cyberspace and the U.S. National Interest," Belfer Center for Science and International Affairs.

11. K. Lord and T. Shrap, "America’s Cyber future Security and Prosperity in the Information Age," Center for a New American Security, vol. 1, 2011.