عصر اطلاعات و تحول مفاهیم جنگ و امنیت در روابط بین‌الملل؛ چگونه دفاع کنیم؟

مهدی شاپوری[۱]، اکرم باقری[۲]

[۱] دانشجوی کارشناسی ارشد روابط بین‌الملل دانشگاه تربیت مدرس

[۲] کارشناس ارشد سیاستگذاری عمومی

shapouri2671@gmail.com

چکیده

این مقاله در پاسخ به این سوال که عصر اطلاعات و گسترش تکنولوژی‌های ارتباطی و اطلاعاتی چگونه باعث تحول مفاهیم جنگ و امنیت در روابط بین‌الملل شده‌است؟ این فرضیه را به آزمون می‌گذارد؛«با گسترش فناوری‌های اطلاعاتی و ارتباطی هم‌اکنون شاهد گذار به دوران جدیدی هستیم که در آن نوع و شیوهٔ جنگ‌ها و در نتیجه مفهوم امنیت متحول شده است. دورانی که در آن فضای جریان‌های شبکه‌ای در یک مجرای نامرئی به تعاملات، انتخاب‌ها و نتایج شکل می‌دهند. بازتولید ابزارهای جنگی سنتی در کنار یا درون یک جریان نامرئی و همچنین تولید ابزارهای پیشرفته و جدید، معمای سنتی امنیت را برای حاکمیت‌ها پیچیده‌تر کرده است به گونه‌ای که احتیاج به یک بازبینی دقیق و همه‌جانبه در مفهوم امنیت توسط دولت‌ها نیازی ضروری است» در فضای سایبر، شبکه‌های گوناگون ارتباطی و اطلاعاتی بهم متصل‌اند. در چنین شرایطی قسمت اعظمی از امور مهم دولتی و بین‌دولتی در زمینه‌هایی همچون تجارت، علم، فرهنگ، سیاست و امنیت از طریق فضای سایبر انجام می‌گیرد. با توجه به آسیب‌پذیری و قابل نفوذ بودن چنین فضایی، اختلال در سامانه آن می‌تواند ضررهای جبران‌ناپذیری به موجودیت‌ها و بازیگران مختلف وارد کند.

واژگان کلیدی:

جنگ سایبری، امنیت سایبری، عصر اطلاعات، فضای شبکه‌ای، روابط بین‌الملل، دفاع سایبری

۱- مقدمه

قابلیت فناوری‌های اطلاعاتی و ارتباطی با ایجاد پیوند میان نظام‌های متنوع و گوناگون فرهنگی، اقتصادی و سیاسی یک دهکدهٔ جهانی را خلق کرده است که در آن به قول کاستلز «مکان و زمان که بنیان‌های مادی تجربهٔ انسانی هستند دگرگون گشته‌اند، چون فضای جریان‌ها[1] بر فضای مکان‌ها[2] چیره گشته و زمان بی‌زمان جایگزین زمان ساعتی دوران صنعتی شده است»[۱] با آمدن الکترون‌ها، داده‌ها و نمابرها و تصاویری که بسرعت در کابل فیبر نوری وارد می‌شوند و از طریق اتصال ماهواره‌ای و ماتریکس فضای سایبر با سرعت نور قابل مشاهده می‌شوند، مرزهای سرزمینی بی‌معنی می‌شود. [۲] در چنین فضایی که پیوستگی‌ها در بسیاری از عرصه‌ها شدت گرفته و در حال نهادینه شدن هستند «اگر همان اشتباه قرن بیستم را مرتکب شویم، یعنی استفاده از تکنولوژی و صنعتی شدن برای قتل عام یکدیگر در جنگ‌های وحشیانه، در آن صورت با قدرت تکنولوژیک جدید چه بسا حیات از روی این کره رخت بربندد»[۳]

اختراع تلفن، رادیو و پس از آن تلویزیون، کامپیوتر، اینترنت و دیگر فناوری‌های نوین اطلاعاتی و ارتباطی باعث ایجاد الگوهای جهانی جدیدی در عرصه‌های ارتباطات، پردازش، ذخیره‌سازی و کاربری اطلاعات شده است. تکنولوژی‌های عصر اطلاعات علاوه بر دگرگونی‌های مثبتی که در بسیاری از جهات مختلف زندگی بشر از جمله؛ شیوهٔ اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، شیوهٔ زندگی و...بوجود آورده‌اند، در بسیاری از موارد می‌توانند به ضرر مالی و حتی جانی کاربرانشان در سطحی محدود یا گسترده ختم شوند. چرا که تکنولوژی‌های نوین در عین حال که به سیستم‌های امنیتی کمک می‌کند، زندگی روزمره را نیز بی‌حفاظ‌تر کرده‌اند. [۴] البته این تعارضات بیش از آنکه ذاتی باشند، ناشی از کاربرد دوگانهٔ این تکنولوژی‌ها توسط انسان است. با اختراع آهن هم گاوآهن ساخته شد و هم شمشیر، با انقلاب صنعتی هم کارخانه‌ها و صنایع پیشرفته ایجاد شدند و هم زرادخانه‌های عظیم تسلیحاتی، انرژی هسته‌ای هم بمنظور تولید برق و داروهای درمانی بکار گرفته می‌شود و هم برای تولید بمب‌هایی که در سطحی وسیع بقای انسان‌ها را به خطر می‌اندازند.

۲- فناوری اطلاعات و روابط بین‌الملل

گسترش و نهادینه شدن شبکه‌های متراکم ارتباطی ناشی از فناوری‌های عصر اطلاعات وضعیتی را در سطح جهان بوجود آورده است که در آن پیوندها و ارتباطات از مجاری جریان‌های مجازی-با شدت، حجم و سرعت خیره‌کننده‌ای-میسر می‌شود. این وضعیت اهمیت زمان و مکان را کمرنگ، امکان ارتباطات گستردهٔ جهانی را تسهیل و همچنین ابعاد و عرصه‌های مختلف زندگی بشری را متحول نموده است. حوزهٔ روابط بین‌الملل نیز از جمله حوزه‌هایی است که از این تغییرات مصون نمانده و تحولات محسوسی در لایه‌های مختلف آن ایجاد شده است. جنگ و امنیت از مهم‌ترین این لایه‌ها محسوب می‌شوند که در این مقاله سعی می‌شود تحول مفهومی و عینی آنها تحت تأثیر تکنولوژی‌های جدید عصر اطلاعات بررسی شود.

امروزه یک شبکهٔ رسانه‌ای کوچک با استفاده از یک وب سایت می‌تواند اسناد مهم سیاست خارجی و امنیت ملی یک کشور را برملا سازد. کارتل‌های بزرگ خبری و تبلیغاتی با پشتوانه‌های مالی و معنوی افراد، گروه‌ها و دولت‌ها می‌توانند مطالبات و خواسته‌های انسان‌ها در اقصی نقاط جهان را یکسان‌سازی، و جهان را تبدیل به یک دهکده کنند. یک هَکِر در روستایی دورافتاده در فیلیپین توانایی حمله به تأسیسات و زیرساخت‌های اطلاعاتی وزارت دفاع آمریکا را پیدا کرده است. با ارسال یک کِرم رایانه‌ای در تأسیسات هسته‌ای یک کشور می‌توان چرنوبیلی دیگر آفرید. با بکارگیری بمب‌های الکترومغناطیسی می‌توان زیرساخت‌های حیاتی مدرن طرف مقابل را با اولین ضربه کاملاً فلج کرد و از کار انداخت. با تلفیق نانوتکنولوژی و سیستم‌های هوشمند اطلاعاتی می‌توان ابزارهایی بسیار کوچک اما با قدرت فوق‌العاده خلق کرد. می‌توان اندازهٔ و وزن موشک‌ها را کاهش و قدرت تخریب آن‌ها را چند برابر کرد. می‌توان با استفاده از حسگرهای نانویی سرعت، دقت و اطمینان بمب‌های مخرب را چند برابر کرد. می‌توان ابزارهای بسیار

1. Space of Flows
2. space of places

ریز جاسوسی خلق کرد به گونه‌ای که نفوذ آن‌ها در هر نقطه‌ای از خاک دشمن امکان‌پذیر باشد.

با این وضعیت، نمی‌توان انکار کرد که توسعه روزافزون فناوری‌های اطلاعاتی و ارتباطی نوع ارتباطات و بسیاری از معادلات محیط روابط بین‌الملل را متحول نموده است. متأثر از این تحولات عینی بسیاری از مفاهیم اساسی نظری حوزهٔ روابط بین‌الملل همچون دیپلماسی، جنگ، صلح، امنیت، حاکمیت، هویت و فرهنگ ملی نیز دچار تحولاتی اساسی شده‌اند. توسعهٔ ارتباطات در اثر انقلاب صنعتی فاصله‌های زمانی و مکانی را تضعیف کرد، اما انقلاب اطلاعات این فاصله‌ها را بطور کلی از بین برد. هم‌اکنون جهان مانند یک دهکدهٔ کوچک یا تار عنکبوت شده است که در آن همه از اوضاع و احوال همدیگر خبر دارند و همه به همدیگر وابسته‌اند بطوریکه در بسیاری از موارد وقوع یک حادثه در دورترین نقطهٔ عالم می‌تواند همگان را درگیر خود سازد.

فناوری‌های ارتباطی و الکترونیکی جدید منجر به بزرگترین بمباران مطالب دیداری و شنیداری شده که بشر در طول تاریخ خود تجربه کرده است. این فناوری‌ها کل جهان را سریع در معرض توجه هر شنونده و بیننده‌ای قرار داده است [۵] بنابراین در عصر اطلاعات هیچکس و هیچ چیزی نمی‌تواند مخفی بماند و هر لحظه - بدون اینکه دولتی به خاک دولت دیگری حمله کرده باشد- احتمال ناامنی وجود دارد. ناامن‌کنندگان امنیت ملی نیز دیگر تنها دولت‌ها نیستند. افراد سودجو، باندهای تبهکار و گروه‌های تروریستی با انگیزه‌های مختلف توانایی به چالش کشیدن امنیت در سطوح گوناگون-شخصی، ملی و بین‌المللی- را پیدا کرده‌اند.

۳- جنگ سایبری

تا قبل از وقوع انقلاب اطلاعات نبردها بصورت فیزیکی و رودرو، و ابزار نبرد نیز محدود به همان سلاح های حاضر در میدان جنگ (در ابتدا ابزارهایی همچون سنگ، شمشیر، چوب و... و بعد از انقلاب صنعتی تفنگ‌ها، توپ‌ها، تانک‌ها، هواپیماها و...) بود. اما به دنبال انقلاب اطلاعات بقول نویسنده‌ای به جزء تفنگ، چاقو، نارنجک و چند مورد دیگر- تعداد کمی سلاح در زرادخانه‌های قرن ۲۱ وجود دارد که به ترانزیستورها، تخته مدار و پردازنده‌ها متکی نباشند. [۶]در جنگ‌های جدید نیازی به تقابل فیزیکی سربازان نیست. «امروزه فضای مجازی میدان نبرد است». با این وضعیت وابستگی به شبکه‌های کامپیوتری تبدیل به یک پاشنه آشیل برای زیرساخت‌های مرتبط با این شبکه‌ها شده است.

هم‌اکنون جنگ‌های سایبری بعد از زمین، دریا، هوا و فضا به بُعد پنجم جنگ تبدیل شده‌اند. [۷] جنگ سایبر به بهره‌برداری از ابزارهای اطلاعاتی(اینترنت)برای ضربه زدن به دیگران از طریق حملهٔ مخفیانه به زیرساخت‌های طرف مقابل گفته می‌شود. [۸] این نوع جنگ‌ها شامل خرابکاری‌ها و اختلال در شبکه‌های کامپیوتری بوسیله هکرهایی است که از جانب حکومتها یا منافع شخصی عمل می کنند. [۹] بر حسب انگیزه، حملات سایبری را می‌توان به دو نوع هدفمند[1] و فرصت‌طلبانه[2] تقسیم کرد. [۱۰] حملهٔ هدفمند اغلب بوسیلهٔ دولت‌ها یا گروه‌های تروریستی و به منظور خاصی مثلاً ضربه زدن به دشمنان یا رقبا هدایت می‌شود، در حالیکه حملهٔ فرصت‌طلبانه بیشتر توسط گروه‌های بزهکار و سارق یا حتی در برخی موارد با انگیزهٔ سرگرمی ترتیب داده می‌شوند. در این میان پیچیدگی، اهمیت و میزان خسارت ناشی از حملات هدفمند بسیار بیشتر از نوع دیگر است چون در اینگونه حملات معمولاً زیرساخت‌های مهم و حیاتی مثل مخابرات، تأسیسات برق، آب و گاز هدف قرار می‌گیرند. با این وجود می‌توان گفت در عصر اطلاعات قدرت بیش از آنکه از لولهٔ تفنگ بیرون بیاید، از دقت‌مندی سیستم‌های و نرم‌افزارهای قوی رایانه‌ای نشأت می‌گیرد. در جنگ‌ها کشورها با استفاده از سیستم‌های رایانه‌ای، اختلالاتی را در سیستمهای اطلاعاتی و ارتباطاتی طرفهای درگیر پدید می‌آورند و با استفاده از سیستم‌های هوشمند دقت سلاح‌ها را افزایش داده و با بکارگیری رادارها و سیستم‌های دفاع موشکی، جنگ‌افزارها و موشک‌های یکدیگر را شناسایی و خنثی می‌کنند.

۴- امنیت سایبری

در برداشت سنتی، امنیت منحصراً در «نبود خطرات فیزیکی» خلاصه می‌شد. در چنین شرایطی اختلال در امنیت به یک حملهٔ

1. targeted
2.opportunistic

فیزیکی بستگی داشت. مثلاً عدم امنیت یا ناامنی تنها زمانی معنا پیدا می‌کرد که سربازان قوم یا کشور "الف" به مرزهای قوم یا کشور "ب" حمله می‌کردند. اما امنیت در معنای نوین را نمی‌توان به تنهایی در چارچوب مرزها و در روابط دولت-ملت‌ها جستجو کرد. امروزه جنگ‌ها همانگونه که جوزف نای می‌گوید خصوصی[1] شده‌اند. [۱۱] گروه‌های تروریستی به یکی از مهمترین چالش‌ها و تهدیدهای امنیت ملی و جهانی مبدل گشته‌اند. آنها با توجه به آسیب‌پذیری مرزها به آسانی می‌توانند به هر نقطه‌ای حمله کنند و نقشه‌های شوم و خرابکارانهٔ خود را در هر مکان به ظاهر امنی پیاده کنند.

امنیت سایبر را می‌توان به استفاده از ابزارهای مرتبط با ایمن‌سازی، توانمندسازی و صحت اطلاعاتی دانست که پردازش، حفاظت و ارتباط‌شان بوسیلهٔ ابزارهای الکترونیکی امکان‌پذیر است. از آنجا که فضای سایبر یک جریان پیوسته و پویاست، حفاظت از اطلاعات در چنین فضایی کار آسانی نیست. تنها ابرقدرت تاریخ مدرن یعنی آمریکا نیز در برابر حملات سایبری آسیب‌پذیر نشان داده است. [۱۲] در جدیدترین سند امنیت ملی آمریکا (تنظیم شده در سال ۲۰۱۰) فضای سایبر در کنار زمین، هوا، دریا و فضا بعنوان یکی از مهمترین حوزه‌های امنیت ملی آمریکا - که لازم است مورد مراقبت و محافظت قرار گیرد - عنوان شده است. (p.22) در این سند (p.27-28) تهدید فضای سایبر بعنوان یکی از چالش‌های جدی برای امنیت ملی، ایمنی عمومی و اقتصاد این کشور بیان شده و آمده است «زیرساخت دیجیتال ما یک دارایی استراتژیک است و حفاظت از آن یکی از اولویت‌های امنیت ملی ماست». [۱۳] در چنین شرایطی منطقی است اگر بگوییم در عصر اطلاعات امنیت به کالایی کمیاب تبدیل شده است چه در سطح خُرد یعنی در رابطه با شهروندان و چه در سطح کلان یعنی در رابطه با دولت-ها. دستگاه‌های اطلاعاتی دولت‌ها و مجرمان اینترنتی با نفوذ و هکِ اطلاعات شخصی شهروندان، حوزهٔ خصوصی را بعنوان محرمانه‌ترین و حیاتی‌ترین حق یک شهروند به چالش کشیده‌اند. «اخاذی اینترنتی» به یک پدیدهٔ رایج تبدیل شده است. پدیده‌ای که به جرأت می‌توان گفت مقابله با آن توسط دولت‌ها سخت‌تر از جنگ‌های معروف کنسرت اروپا علیه جاه‌طلبی‌های ناپلئون در اوایل قرن ۱۸ است. چرا که نه مبدأ حمله کاملاً روشن، و نه مقصد آن قابل پیش‌بینی است.

فرصت‌ها و خطرات ناشی از فضای سایبر در قرن ۲۱ به یکی از دغدغه‌های اساسی کشورهای صنعتی و پیشرفته تبدیل شده، به گونه‌ای که تقریباً اکثر این کشورها به تنظیم سند امنیت سایبری برای استفاده از مزیت‌های این فضا و مقابله با چالش‌های ناشی از آن پرداخته‌اند. در سند «استراتژی امنیت سایبری آلمان» (تنظیم شده در سال ۲۰۱۱) آمده است «تضمین امنیت فضای سایبر به یک چالش کلیدی برای دولت، جامعه و تجارت در هر دو سطح ملی و بین‌المللی تبدیل شده است...از آنجا که سیستم‌های فناوری اطلاعات در شبکه‌های گستردهٔ جهانی بهم متصل‌اند، اتفاق‌ها در زیرساخت‌های اطلاعاتی دیگر کشورها ممکن است بصورت غیرمستقیم بر آلمان نیز تأثیر بگذارد. به همین دلیل تقویت امنیت فضای سایبر نیاز به ایجاد قواعد، استانداردها و نُرم‌های بین‌المللی دارد که این مهم نیز همکاری نزدیک میان دولت‌ها در سطح جهان را می‌طلبد» [۱۴] شعار سند امنیت سایبری انگلستان بر «کاهش ریسک‌های فضای سایبر و بهره‌برداری از فرصت‌های آن با بهبود دانش، توانایی‌ها و تصمیم‌گیری‌ها» مبتنی است. در سند مذکور آمده است «همانگونه که در قرن ۱۹ دریاها و در قرن ۲۰ فضا را به منظور ایمنی و کامیابی ملی‌مان امن نگه داشتیم، در قرن ۲۱ نیز باید فضای سایبر را برای برخورداری از مزیت‌های آن امن نگه داریم»[۱۵] هدف سیاست امنیت سایبری استرالیا اینگونه بیان شده است: «حفظ یک فضای الکترونیکی امن، آرام و مطمئن که امنیت ملی و منفعت‌های اقتصاد دیجیتالی را ارتقا می‌دهد»[۱۶]

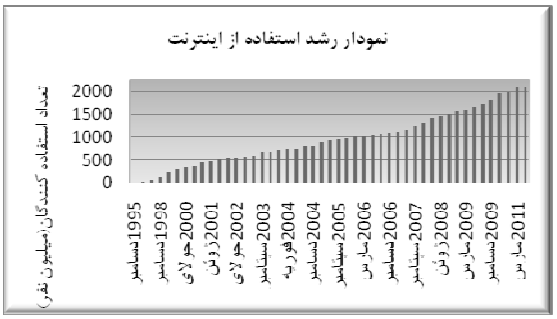
۵- اینترنت به عنوان مهم‌ترین منبع تهدید سایبری

دسترسی به اینترنت بعنوان منبع اصلی تهدید سایبر به طور روزافزونی در حال افزایش است.(بنگرید به جدول و نمودار الف) اینترنت به نحوی شگفت‌آور ماهیت روابط اجتماعی درون و میان ملت‌ها را بازتعریف کرده است. محیط مجازی و جامعه‌های اطلاعاتی در سراسر جهان رو به گسترش‌اند و این امر از تأکید و

3. privatization of war

اهمیت زمان و مکان کاسته است. با تبدیل اینترنت به وسیلهٔ روزمره و قابل دسترس از هر نقطهٔ جهان، واحدهای جغرافیایی که از لحاظ زمانی و مکانی از هم جدا شده‌اند هر چه بیشتر به انواع روابط اطلاعاتی متصل شده‌اند.

از سال ۲۰۰۰ تا ۲۰۱۰ میزان دسترسی و استفاده از اینترنت از ۳۶۰ میلیون نفر در جهان به ۲ میلیارد نفر رسیده است. وزارت دفاع آمریکا به تنهایی دارای ۱۵ هزار شبکه و ۷ میلیون دستگاه کامپیوتری در مناطق مختلف جهان می‌باشد. [۱۷] طبق برآوردهای وزارت دفاع آمریکا، وابستگی‌های این دپارتمان به شبکه‌ها برای فرماندهی و کنترل نیروها، لجستیک، عملیات‌های جاسوسی و توسعهٔ تکنولوژی‌های تسلیحاتی اغراق نیست. چرا که در قرن ۲۱ نیروهای مسلح را نمی‌توان بدون انعطاف‌پذیری، اطلاعات قابل اعتماد و شبکه‌های ارتباطی که فضای سایبر دستیابی به آنها را تضمین می‌کند با سرعت و دقت بالا هدایت و فرماندهی کرد. [۱۸] لئون پانِتا رئیس سابق سازمان سیا و وزیر فعلی دفاع آمریکا معتقد است «یک پرل هاربور یا ۱۱ سپتامبر دیگر می‌تواند در فضای سایبر اتفاق بیافتد»[1] معاون وزارت دفاع آمریکا نیز برآنست که «در قرن ۲۱ بیت و بایت همچون گلوله و بمب تهدیدکننده هستند» استدلال وی برآنست که هم‌اکنون بیش از ۳۰ کشور در حال ایجاد و توسعهٔ واحدهای نظامی سایبری هستند که این اقدامات و پیشرفت‌ها نمی‌تواند صرفاً دفاعی فرض شود. [۱۹]



Source: http://www.internetworldstats.com/emarketing.htm

۶- مشخصه‌های حملات سایبری

نامشخص ماندن هویت و مکان حمله کننده: در جنگ‌های سایبری کشف هویت و مکان حمله‌کننده بسیار دشوار است. در ۱۹۹۸ وزارت دفاع امریکا مورد حملات سایبری قرار گرفت. در این حمله گروهی از هکرها صدها شبکه کامپیوتری ناسا، پنتاگون و سایر آژانس‌های امنیتی و دفاعی را مختل کردند. بعد از بررسی های انجام شده ریشه‌های این حمله در کشور روسیه کشف شد. اما کاملاً روشن نبود که آیا از سوی دولت این کشور بوده است یا خیر. علی‌رغم تمام تلاشهای تحقیقاتی، امریکا هنوز نتوانسته است بفهمد که چه کسی پشت این حملات بوده است. [۲۰]

راحت و ارزان بودن اینگونه حملات: تنها مواد لازم برای تبدیل شدن به یک جنگجوی اطلاعاتی دسترسی به کامپیوتر، امکانات اینترنتی و میزانی از توانایی و دانش استفاده از این ابزار است که با توجه به گستردگی و رواج پیشرفته‌ترین و جدیدترین مدل‌های کامپیوتر و نرم افزار، این ابزار در هر کجا و برای هر کسی در دسترس است.

سهولت فرار از جُرم: اولاً: یک هَکِر برای حمله و ایجاد خرابکاری در یک شبکهٔ کامپیوتری لزومی ندارد از شبکه یا ابزارهای شخصی و خانگی برای این منظور استفاده کند. او می‌تواند از محل‌های عمومی برای عملی ساختن نیات خود بهره بگیرد. ثانیاً: یک گروه تروریستی مثل القاعده با یک شبکهٔ گسترده در کشورهای مختلف را به هیچ وجه نمی‌توان تحت تعقیب قرار داد. ثالثاً: در قوانین بسیاری از کشورهای دنیا جُرم سایبری یک جُرم ناشناخته است و قانونی برای برخورد با مجرمین در این زمینه وجود ندارد.

غیرقابل پیش‌گیری بودن حملات سایبری: مثلاً در سال ۱۹۹۷ برای تخمین میزان آسیب پذیری سیستم نظامی امریکا شبیه سازی‌هایی صورت گرفت. به این صورت که فرض شد یک بحران نظامی در شبه جزیره کره رُخ داده است. به این ترتیب هکرهایی با استفاده از برنامه‌های اینترنتی به خراب کردن سیستم‌ها و شبکه‌های کامپیوتری در چند شهر امریکا پرداختند. نتیجهٔ این شبیه‌سازی نشان داد هکرهای واقعی می توانند با استفاده از شبکه‌های کامپیوتری بدون هیچگونه واکنش موثر برای جلوگیری از آنها، عملیات خرابکارانه انجام دهند. [۲۱]

1. “Panetta Praises Nation’s Unity on 9/11”, Sept. 9, 2011, at: http://www.defense.gov/news/newsarticle.aspx?id=65289

با این وضعیت، در حال حاضر بحث حملات سایبری، دفاع سایبر و امنیت سایبر بعنوان موضوعاتی مهم در دپارتمان اطلاعاتی و دفاعی بسیاری از کشورها مخصوصاً کشورهای پیشرفته مطرح است. با توجه به مشکل بودن شناسایی هویت و مکان مهاجم، راحت و ارزان بودن حمله، سهولت فرار از جُرم و غیرقابل پیش‌گیری بودن حملات سایبری می‌توان گفت چالشی که این فضا برای امنیت ملی دولت‌ها ایجاد کرده از همهٔ انواع چالش‌های سابق امنیت ملی مهمتر و پیچیده‌تر هستند. جنگ‌های سایبری دیگر تمرکز بر مرزها و مناقشات سرزمینی نیست و حفظ امنیت ملی نیز تنها منوط به محفوظ نگه داشتن مرزها نیست. این اشکال جدید از جنگ‌ها تعریف و مفهوم سنتی امنیت را دگرگون کرده‌اند. چرا که در چنین جنگ‌هایی نه بحث سازماندهی مطرح و لازم است و نه لزوماً خبری از کشت‌وکشتار و خونریزی. استراتژی اصلی در جنگ‌های سایبری «محو و نابودی دشمن بدون جنگیدن» است که دو میلیون سال پیش توسط سون‌تزو (استراتژیست معروف چینی) مطرح شده بود. [۲۲]

۷- چگونه دفاع کنیم؟

چند راه برای مقابله با تهدیدات سایبری وجود دارد. از جمله مهمترین این راه‌ها می‌توان به سه مورد اشاره کرد: ۱.همکاری نزدیک میان بخش‌های مختلف جامعه؛ ۲.ایجاد رژیم‌ها و نهادهایی در سطح بین‌الملل؛ ۳.گسترش حوزهٔ نفوذ و اقدامات دولت‌ها به منظور نظارت و کنترل بیشتر بر این فضای نامرئی. دربارهٔ مورد اول باید گفت به دلیل خصلت غافلگیرانهٔ حملات سایبری و گستردگی کارگزاری‌های مختلف در جامعه، در عمل ایجاد هماهنگی کامل میان بخش‌های مختلف امکان‌پذیر نیست. دربارهٔ مورد دوم نیز می‌توان گفت از آنجا که ساختار نظام بین‌الملل آنارشیک است و همه دولت‌ها بدنبال افزایش قدرت و بهینه ساختن امنیت خود هستند، هر لحظه امکان تقلب وجود دارد. در اینجا دیگر بحث سایهٔ آینده[1] مطرح نیست، چرا که هر دولتی می‌تواند به دیگری ضربه بزند و در مقام پاسخگویی منکر همه چیز شود. در چنین شرایطی، به عقیده نگارندگان این مقاله بهترین راهکار «گسترش قدرت دولت‌ها در این حوزه و ایجاد فرماندهی واحد برای برخورد با خطرات در مواقع اضطراری است». در این راستا به نظر می‌رسد در دست داشتن «کلید انسداد ملی» توسط تمام دولت‌ها گزینهٔ نسبتاً مناسبی باشد، همانگونه که هم‌اکنون آمریکا از این امتیاز در سطحی گسترده برخوردار است.

در سال ۲۰۱۰ سه سناتور آمریکایی، «جو لیبرمن»، «سوزان کالینز» و «تام کارپر» لایحه‌ی«قانون حمایت از فضای سایبری به عنوان یک دارایی ملّی» را به سنا ارائه کردند که کلید انسداد[2] نام دارد. این لایحه که به تصویب سنا نیز رسید به رئیس جمهور آمریکا اجازه می‌دهد تا در شرایطی که امنیت سایبری آمریکا به خطر می‌افتد به موتورهای جستجوگر اینترنتی مانند یاهو و گوگل دستور تعلیق دسترسی کامل کاربران به سرویس‌های اینترنتی این موتورهای جستجوگر را صادر کند. لیبرمن ریاست کمیسیون امنیت ملی سنا و طراح اصلی این لایحه در همین راستا گفت :«یک حمله سایبری به آمریکا می‌تواند همچون یک حمله جنگی یا بیش از آن به بانک‌ها، ارتباطات، مالیه و حمل و نقل ما آسیب برساند[3].»

۸- نتیجه‌گیری

در این مقاله به بررسی تأثیر فناوری‌های نوین اطلاعاتی-بخصوص اینترنت- بر دو حوزهٔ جنگ و امنیت در روابط بین‌الملل و همچنین بهترین راهکارهای دفاعی دولت‌ها برای برخورد با تهدیدات سایبری پرداخته شد. یافته‌های تحقیق نشان می‌دهد گسترش ابزارها و فناوری‌های اطلاعاتی و ارتباطاتی جدید، نوع و شیوهٔ جنگ‌ها و تهدیدها برای دولت‌های ملی را دگرگون ساخته است که در نتیجهٔ آن معمای امنیت نیز - برای حاکمیت‌ها - پیچیده‌تر شده است. از نظر نگارندگان بهترین شیوهٔ برخورد با خطرات جدید، کنترل بیشتر دولت‌ها بر فضای سایبر است.

1. shadow of future

2. kill switch

1. Joe Lieberman: China can shut down the Internet, why can't we? Available in http://original.antiwar.com, and Obama 'Internet kill switch' plan approved by US Senate panel at: http://news.techworld.com/security/3228198/obama-internet-kill-switch-plan-approved-by-us-senate-panel/

منابع

۱. کاستلز، مانوئل، عصر اطلاعات؛ جامعه، اقتصاد و فرهنگ(جلد سوم)، ترجمه احد علیقلیان،افشین خاکباز و علی پایا(ویراستار)، طرح نو، ۱۳۸۰، ص۱۳

۲. ابو، بوسا، امپریالیسم سایبر : روابط جهانی در عصر جدید الکترونیک، ترجمه پرویز علوی، نشر ثانیه، ۱۳۸۵، ص۴۱۶

۳. کاستلز، همان، ص۴۳۶

۴. کاستلز، همان، ص۴۴۰

۵. روزنا، جیمز، آشوب در جهان سیاست، ترجمه علیرضا طیب، تهران روزنه، ۱۳۸۳، ص۴۵۴

6. Knowles, John, Warfare: E-Bombs, 2003 at: http://www.pcmag.com/article
7. The Economist (2011), Cybersecurity in America and Europe: Freedom and security in cyberspace, at: http://www.economist.com/blogs/charlemagne/2011/10/cybersecurity-america-and-europe
8. Lewis, James A. (2002), Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies
9. Adams, James (2001), "Virtual Defense," Foreign Affairs, vol. 80, no. 3
10. GFI Software, Targeted cyber attacks: The dangers faced by your corporate network, 2009, www.gfi.com
11. Nye, Joseph, THE PARADOX OF AMERICAN POWER (lecture), edited by Robertson Hall, Princeton University, May 8, 2002
12. Adams, op.cit.
13. US National Security Strategy, with house, May 2011, www.whitehouse.gov/sites/default/.../National _security_strategy.pdf
14. Cyber Security Strategy for Germany, Federal Ministry of the Interior, 2011
15. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, Presented to Parliament by the Prime Minister, by Command of Her Majesty June 2009, Crown Copyright 2009
16. Australian Cyber Security Strategy Commonwealth of Australia 2009, at: www.acs.org.au/index.cfm?action=show&conID...
17. US Cyber Strategy, Department of Defense Strategy for Operating in Cyberspace, July 2011
18. US Quadrennial Defense Review Report, Secretary of Defense, Washington DC 20301-1000, February 2010
19. Lynn III, William J., “The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack”,http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later
20. Adams, op.cit.
21. Adams, Ibid.
22. Wriston, W.B., (1997, September/October), “Bits, Bytes and Diplomacy”, Foreign Affairs

This page is intentionally left blank