فصلنامه دانش سیاسی و بین‌الملل
سال دوم، شماره پنجم، بهار۱۳۹۲
تاریخ وصول: ۱۳۹۱/۰۶/۲. تاریخ پذیرش: ۱۳۹۱/۱۱/۲۹
صص ۲۰ - ۱

جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات متحده آمریکا

احمد جالینوسی[۱]، شهروز ابراهیمی[۲]*، طیبه قنواتی[۳]

۱- استادیار روابط بین الملل دانشگاه اصفهان
۲- استادیار روابط بین الملل دانشگاه اصفهان
۳- کارشناس ارشد روابط بین الملل از دانشگاه اصفهان

چکیده

تهدیدهای و حملات سایبری در استراتژی امنیت ملی آمریکا جایگاه پر اهمیتی دارد. اگر چه جنگ سایبری به معنای واقعی آن تا حال حاضر صورت نگرفته است، ولی حملات روزانه سایبری حکایت از چشم‌انداز مخوف جنگ سایبری در آینده دارد. از این رو ایالات متحده با در نظر گرفتن این امر و این که یک جنگ سایبری اگر به وقوع بپیوندد تلفات و خطرات آن کمتر از جنگ کلاسیک نخواهد بود، دست به طرح‌ها و ابتکارهای نهادی مختلفی دراین زمینه زده است و استراتژی امنیت ملی آمریکا به نوعی دچار دگرگونی شده است. هدف مقاله تبیین فضای سایبر، حملات و تهدیدهای سایبری و جایگاه آن در استراتژی امنیت ملی آمریکاست. سوال اصلی نوشتار این است که فضای سایبر در استراتژی امنیت ملی آمریکا چه جایگاهی دارد؟ فرضیه اصلی مورد آزمون در پاسخ به سوال این است که با توجه به اهمیت فضای سایبر در ایالات متحده و خطرات آینده ناشی از حملات سایبری دشمن، آمریکا در استراتژی امنیت ملی خود بازنگری نموده و بعد فضای سایبر را- به عنوان بعد پنجم- به ابعاد سنتی تهدیدهای (ابعاد چهارگانه زمین، دریا، هوا و فضا) افزوده است. فرضیه فرعی نوشتار این است که اگر چه تا حالا جنگ سایبری به معنای واقعی کلمه صورت نگرفته، ولی حملات روزانه سایبری (متفاوت با جنگ سایبری) چشم‌انداز مخوفی از جنگ سایبری ارایه می‌دهد و در استراتژی امنیت ملی آمریکا خطرات جنگ سایبری در صورت وقوع به همان اندازه یک جنگ کلاسیک می‌تواند رفاه و امنیت شهروندان را بطور جبران ناپذیری به خطر اندازد. مفروض نوشتار این است که عمده‌ترین تهدید جنگ سایبری در صورت وقوع، تخریب زیر ساخت‌های حساس است که تماماً و بیش از پیش در حال ابتنای بر فضای سایبری هستند. مقاله با روش توصیفی- تحلیلی، با ابزار کتابخانه‌ای و

* نویسنده مسؤول Ebrahimi_Shahrooz@yahoo.com

براساس مبانی نظری "بعد جدید قدرت در چارچوب فضای سایبر" به رشته تحریر درآمده است.
واژه‌های کلیدی: قدرت، فضای سایبر، حمله سایبری، جنگ سایبری، ایالات متحده آمریکا، استراتژی امنیت ملی آمریکا.

مقدمه

«همانند مرزهای فیزیکی ایالات متحده، مرزهای سایبری نیز بسیار نفوذ پذیر هستند و به تبع، زیرساخت‌های حساس ایالات متحده که اقتصاد این کشور بسیار به آن وابسته است می‌تواند هدف بازیگران غیردولتی و دولتی قرار بگیرد. برتری جهانی کنونی آمریکا ضامن مصونیت آمریکا از چنین خطراتی نیست».

دان کاولتی،۱۳۸۹:۱۴۸-۱۴۷

قدرت در زمینه معنا می‌یابد، و رشد سریع فضای سایبر زمینه‌ای جدید و مهم در سیاست جهان است. هزینه پایین ورود، گمنامی، و نامتقارن بودن در آسیب‌پذیری، بدین معناست که بازیگران کوچک‌تر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت سخت و نرم دارند. تغییرات به وجود آمده در اطلاعات همیشه تأثیر مهمی بر قدرت داشته‌اند، اما حوزه سایبر یک محیط مصنوعی جدید و غیرقابل پیش‌بینی است. ویژگی‌های فضای سایبر برخی از اختلاف‌های قدرت بین بازیگران را کاهش داده و بدین ترتیب مثال خوبی از پراکندگی قدرت را که ویژگی سیاست جهانی در قرن حاضر است، به نمایش می‌گذارد. قدرت‌های بزرگ نخواهند توانست به اندازه حوزه‌هایی چون دریا و خشکی بر این حوزه مسلط شوند (نی، ۲۰۱۰: ۱).

در سال ۱۸۹۰، «آلفرد تایر ماهان»[1] اهمیت قدرت دریایی را در زمینه فن‌آوری‌های جدید موتور بخار، زره و توپ‌های دوربرد برجسته ساخت. در سال ۱۹۰۷ «تئودور روزولت» نیروی دریایی آب‌های آزاد خود را به شکل قابل‌توجهی گسترش داده و آن را به سراسر جهان گسیل نمود. در اوایل قرن بیستم، «گولیودوهه»[2] ژنرال ایتالیایی اولین کسی بود که نظریه ضرورت قدرت هوایی برای برتری نظامی را مطرح کرد. پس از معرفی هواپیما در جنگ جهانی اول، نظامیان شروع به نظریه‌پردازی در مورد حوزه قدرت هوایی و قابلیت آن برای حمله مستقیم به مرکز ثقل شهری دشمن بدون نیاز به عبور ارتش از مرزها کردند. سرمایه‌گذاری‌های فرانکلین روزولت در قدرت هوایی در جنگ جهانی دوم حیاتی بود. پس از ساخت موشک‌های قاره‌پیما و ماهواره‌های شناسایی و مخابراتی در دهه ۱۹۶۰، نویسندگان شروع به نظریه‌پردازی در مورد حوزه مخصوص قدرت فضایی نمودند. «جان اف‌کندی» برنامه‌ای را آغاز کرد تا از پیشگامی آمریکا در فضا مطمئن شده و یک انسان را به ماه بفرستد (نی، ۲۰۱۰: ۴).

در همین خصوص آمریکا اولین کشوری بود که علاوه بر سایر میادین جنگ نظامی از جمله زمین، دریا، هوا و فضا به فضای مجازی نیز به مثابه محیط جدیدی برای عملیات نظامی نزدیک شد. این مفهوم به سال ۱۹۹۸ برمی‌گردد اما پس از وقوع جنگ اوت ۲۰۰۸ در اوستیای جنوبی به یک طرح واقعی تبدیل شد که البته لازم به ذکر است نتوانست نقش خود را

1 Alfred Thayer Mahan

2 GiulioDouhet

برای آمریکا و متحد واشنگتن در منطقه یعنی گرجستان به خوبی ایفا نماید (www.khabarfarsi.com).

به طور کلی، همانگونه که ریچارد کلارک[1] استدلال می‌کند، جنگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به طور کامل درک کنیم. اما روشن است در دنیای امروز میدان جنگ حوزه خود را به فضای مجازی گسترش داده است و باید آن را به عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین، هوا، دریا و فضا یاد کرد (کورنیش و همکاران، ۲۰۱۰: ۱۲ و ۱۳).

حتی کشورهای بزرگی مانند آمریکا، که منابع عظیمی از قدرت سخت و نرم در اختیار دارند، خود را در حال تقسیم عرصه با بازیگران جدید و مواجه شدن با مشکلات بیشتر در کنترل مرزهایشان در حوزه سایبر می‌یابند. فضای سایبر جای فضای جغرافیایی را نخواهد گرفت و حاکمیت دولت را منسوخ نخواهد ساخت، اما پراکندگی قدرت در فضای سایبر وجود خواهد داشت و اعمال قدرت در هر یک از این ابعاد را به شدت پیچیده خواهد ساخت (نی، ۲۰۱۰: ۳).

در سال ۲۰۰۹، «باراک اوباما» خواستار یک پیش-قدمی بزرگ و جدید در زمینه قدرت سایبری شد و کشورهای دیگر نیزاین رویه را پیش گرفته‌اند. به محض اینکه تغییرات تکنولوژیکی حوزه‌های قدرت را تغییر می‌دهند، رهبران سیاسی نیز با آن همراهی می‌کنند،حوزه سایبر نیز از این نظر حوزه‌ای منحصر به فرد است که هم مصنوعی و جدید بوده و هم به مراتب سریع‌تر از محیط‌های دیگر در معرض تغییرات تکنولوژیکی است. جغرافیای فضای سایبر بسیار ناپایدارتر از محیط‌های دیگر است. جابجا کردن کوه‌ها و دریاها مشکل است، اما با فشردن یک کلید می‌توان بخش‌هایی از فضای سایبر را خاموش و روشن کرد. گسیل کردن الکترون‌ها به سراسر جهان ارزان‌تر و سریع‌تر از جابجایی کشتی‌های بزرگ در فواصل طولانی است (نی، ۲۰۱۰: ۴).

ایالات متحده آمریکا که از نخستین کشورهای تهاجم سایبری محسوب می‌شود، اخیراً اعلام کرده است از بودجه نظامی خود خواهد کاست،اما در بودجه سال ۲۰۱۲ خود ۳/۲ میلیون دلار را برای ارتقای قابلیت‌های سایبری خود اختصاص داده است که در مقایسه با سال مالی ۲۰۱۱ با رشد ۲ درصدی همراه خواهد بود و همچنین دستور مستقیم رئیس جمهور ایالات متحده آمریکا را برای حمله به کشورهای مخالف سیاست‌های این کشور به دنبال داشته است (لرد و شارپ، ۲۰۱۱: ۳۴).

تهدیدهای سایبری قابل پیش‌بینی حال و آینده آمریکا را تهدید می‌کند. این تهدیدها که پیشرفت‌های نظامی، اجتماعی و اقتصادی ایجاد شده توسط دنیای سایبری را به مخاطره انداخته، نه تنها مختص به آمریکا، بلکه به تمام دنیا مربوط است. این تهدیدها به چالشی جدی در زمینه امنیت داخلی آمریکا تبدیل شده و نیازمند توجه بیشتر سران آمریکایی است.

سوال اصلی نوشتار این است که فضای سایبر و تهدیدهای سایبری چه جایگاهی در استراتژی امنیت ملی آمریکا ایفا می‌کند؟ فرضیه اصلی به شرح ذیل برای پاسخ به سوال اصلی مورد آزمون قرار گرفته است: با توجه به اهمیت فضای سایبر در ایالات متحده و خطرات آینده ناشی از حملات سایبری دشمن، آمریکا در استراتژی امنیت ملی خود بازنگری نموده و بعد فضای سایبر را به ابعاد سنتی تهدیدهای

1 Ricghardclarke

(ابعاد چهار گانه زمین، دریا، هوا و فضا) افزوده است. فرضیه فرعی دیگر این که اگر چه تا حالا جنگ سایبری به معنای وافعی کلمه صورت نگرفته، ولی حملات روزانه سایبری (متفاوت با جنگ سایبری) چشم‌انداز مخوفی از جنگ سایبری ارایه می‌دهد ودر استراتژی امنیت ملی آمریکا خطرات جنگ سایبری در صورت وقوع به همان اندازه یک جنگ کلاسیک می‌تواند رفاه و امنیت شهروندان را بطور جبران ناپذیری به خطر اندازد. مفروضات نوشتار به شرح ذیل است:

۱- امنیت سایبری برای حمایت و پیشبرد منافع ملی آمریکا اهمیت حیاتی دارد. ۲- بسیاری از زیر ساخت‌های حساس وابسته به امنیت سایبری هستند.۳- تهدیدهای سایبری و چالش‌های مربوط به آن، باعث شده که آمریکا در دوره جرج بوش پسر و باراکاوباما دست به ابتکارهای نهادی از جمله تأسیس وزارت امنیت داخلی بزند.۴- پس از ۱۱ سپتامبر- با توجه به این که حمله کنندگان به برج‌های دوقلو از ابزارهای جدید اینترنتی جهت هماهنگی اقدامات خود استفاده نمودند- تهدیدهای سایبری در مرکز توجه طراحان امنیت ملی آمریکا قرار گرفته است.

سازماندهی نوشتار به شرح ذیل است. در قسمت اول به معرفی مبانی نظری پرداخته شده است. در قسمت دوم به این امر رداخته شده است که چگونه زیر ساخت‌های حساس جامعه که رفاه شهروندان آمریکا و امنیت ملی به آنها وابسته است هر چه بیشتر وابسته به فضای سایبر شده‌اند و هر گونه تهدیدهای حمله سایبری و به ویژه جنگ سایبری می‌تواند به تخریب این زیر ساخت‌ها منجر شده ودر کنار مخاطره قرار گرفتن رفاه شهروندان، بطور غیر مستقیم جان شهروندان هم می‌تواند در مخاطره قرار گیرد. در قسمت‌های سوم و چهارم به طرح‌ها و ابتکارهای نهادی که آمریکا برای مقابله با تهدیدهای سایبری تدارک دیده است پرداخته می‌شود.

چارچوب نظری: تحول مفهوم وامنیت قدرت درفضای سایبر

دو نوع جابجایی قدرت در این قرن در حال رخ دادن است: انتقال قدرت، و انتشار قدرت. انتقال قدرت از یک کشور مسلط به کشوری دیگر، یک رویداد آشنای تاریخی است، اما انتشار قدرت، یک فرایند جدیدتر است. مشکل همه ممالک در عصر اطلاعات کنونی این است که امور بیشتری خارج از کنترل حتی قوی‌ترین ممالک در حال رخ دادن است. به قول یکی از مدیران سابق وزارت خارجه در برنامه ریزی سیاستی: «اشاعه اطلاعات به همان میزان باعث رفع وضعیت تک قطبی است که گسترش سلاح» (نی، ۲۰۱۰: ۴). فضای سایبر و فناوری‌هایی که استفاده از این فضا را برای ما ممکن می‌سازد به تمام مردم جهان از هر ملیت، نژاد، دین و دیدگاه اجازه می‌دهد تا با یکدیگر ارتباط برقرار کرده، همکاری کنند و به پیشرفت و شکوفایی برسند. امروزه یک شرکت آمریکایی می‌تواند در هر نقطه از جهان از طریق ارتباطات اینترنتی به تجارت بپردازد، از مشاغل بی‌شماری حمایت به عمل آورد و فرصت‌های مناسبی را در اختیار مردم آمریکا قرار دهد (لرد و شارپ، ۲۰۱۱: ۳).

فضای سایبری فراهم‌کننده رابطه‌ای است که در آن مردم بی‌نیاز از اتکا بر روابط چهره به چهره می‌توانند دست به تعامل و هماهنگی اقداماتشان بزنند (کاراز و جیانی، ۵:۱۳۸۸).

فضای سایبر محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع و فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابه‌جایی‌های فیزیکی نیست و همه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس[1] صورت می‌گیرد. فضای سایبر، به معنای مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی، بدون در نظر گرفتن جغرافیای فیزیکی،گفته می‌شود (سلیمانی فارسانی، ۴۱:۱۳۸۸).

ماهیت فضای سایبر، ماهیتی فرا فیزیکی و غیرملموس است و به‌طور کلی، متفاوت با ماهیت فضای سنتی است. با توسعه فضای سایبر، مفاهیم و اصطلاحاتی در ادبیات الکترونیکی جهان رایج گردید که اساس خود را از فعالیت‌ها و توسعه بیشتری در فضای فیزیکی به عاریه گرفت. برخی از آنها عبارت-اند از: دولت الکترونیکی، تجارت الکترونیکی، جنگ سایبر و. (دی آنجلیز، ۶۰:۱۳۸۳). فضای سایبر، شبکه‌های رایانه‌ای و مخابراتی متصل به هم است که اطلاعات را در کمترین زمان و بیشترین مکان، مبادله می‌کند، در نتیجه بارزترین ویژگی فضای سایبر، دسترس پذیر ساختن سریع و با حداقل هزینه همه اطلاعات «آن لاین[2]» است (جلالی فراهانی، ۸۶:۱۳۸۵). و از ویژگی‌های دیگر آن می‌توان جهانی و فرامرزی بودن، دستیابی آسان به آخرین اطلاعات نام برد (سلیمانی فارسانی، ۴۱:۱۳۸۸).

قدرت مبتنی بر منابع اطلاعات، امری تازه نیست، اما قدرت سایبری چیز تازه‌ای است. ده‌ها تعریف از فضای سایبری وجود دارد به‌طور کلی، سایبر، پیشوندی است که به معنی فعالیت‌های الکترونیکی و رایانه‌ای است. براساس یکی از تعاریف: «فضای سایبری عبارت است از یک حوزه عملیاتی که چارچوب آن به‌واسطه استفاده از علم الکترونیک برای... بهره‌کشی از اطلاعات از طریق سامانه‌های متصل به هم و زیرساخت‌های مرتبط با آن تعیین می‌شود» (کهل، ۲۰۰۹: ۲۶ تا ۲۸). فضای سایبری از سوی برخی کارشناسان به عنوان «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی و یا کاربران آن شکل می‌گیرد» تعریف شده است (لرد و شارپ، ۲۰۱۱: ۱۰). پسوند سایبر که خود این واژه از واژه کاربرد از «طریق کامپیوتر» اخذ شده است: سایبرنتیک عبارت است از تئوری ارتباط‌ها و کنترل منظم بازخوردهایی که ارتباط وکنترل موجودات زنده و ماشین‌های دست ساز بشر را بررسی می‌کند. سایبرنتیک را طلیعه‌دار تفکر پیچیده در پرسش و جستجو از سامانه‌های فعال با کاربرد مفاهیم بازخوری و کنترلی نیز می‌دانند. تک واژه «سایبری»حتی امروزه به نظر می‌رسد که دیگر هیچ پیوند مستقیمی با ریشه‌های خود نداشته باشد و بیشتر به نوعی تفکر نظام‌مند متصل است. مفهوم «سامانه‌ها» قطعاً در بستر تهدیدهای سایبری، مفهومی اصلی و مرکزی است و دارای پیامدهای رویه‌ای و تئوریکی متعددی برای چگونگی برخورد و بررسی موضوع است (دان کاولتی،۲۶:۱۳۸۹).

گاه فراموش می‌کنیم فضای سایبری جدید چگونه است. در ۱۹۶۹ وزارت دفاع آمریکا یک اتصال محدود و جزیی را بین چند رایانه‌ی معدود راه‌اندازی

1 Mouse
2 On Line

کرد،که آرپانت[1] نامیده می‌شد، و در ۱۹۷۲ کدهای تبادل داده‌ها به منظور ایجاد یک اینترنت ساده که قادر به تبادل بسته‌های داده‌ای اطلاعات دیجیتالی بود، ایجاد گردید. نظام نام‌های دومین آدرس‌های اینترنتی در ۱۹۸۳ آغاز به کار کرد و اولین ویروس‌های رایانه-ای نیز حدوداً در همان زمان ایجاد شد. شبکه جهانی اینترنت در ۱۹۸۹ به راه افتاد، گوگل[2] (محبوب‌ترین موتور جست‌وجو) در ۱۹۹۸ تأسیس گردید، و دانشنامه منبع باز و یکی پدیدار ۲۰۰۱ راه‌اندازی شد. در اواخر دهه ۱۹۹۰ کسب و کارها شروع به استفاده از این فناوری جدید برای جابجایی تولید و عرضه کالا در زنجیره‌های پیچیده عرضه جهانی نمودند (نی، ۱۹۴:۱۳۹۰).

از منظرجوزفنای، «قدرت سایبری»عبارت است از توانایی به دست آوردن نتایج مورد نظرازطریق استفاده ازمنابع اطلاعات به‌هم پیوست‌های الکترونیک دردامنه‌ها مجازی. قدرت سایبری برای پیگیری اهداف در فضای مجازی یا اهداف درخارج ازاین حوزه مورد بهره‌برداری

تعریف زیرساخت حیاتی

ما بیشتر توانمندی گسترده‌ای را برای بهره‌برداری از آسیب پذیری‌های زیرساختی به دست آوردیم. توانایی ایجاد صدمه «بویژه از طریق شبکه‌های اطلاعاتی» توانایی واقعی است، این توانمندی با سرعتی هشدار دهنده در حال رشد است، و این در حالی است که ما توان دفاعی محدودی در اختیار داشتیم (کمیسون رییس جمهور در مورد حفاظت در زیرساخت‌های حیاتی) (دان کاولتی، ۱:۱۳۸۹).

در اولین گام باید مشخص شود که به چه چیزهایی زیرساخت‌های حیاتی[3] اطلاق می‌شود. در پاسخ به این سؤال ابتدا می‌توان تعاریفی که تاکنون از این مفهوم ارایه شده را مورد بررسی قرار داد.

واژه نامه آمریکن هریتیج[4] در تعریف زیرساخت به تسهیلات، خدمات و تأسیس‌های مورد نیاز کارآمد، از جمله: سیستم‌های حمل‌ونقل و ارتباط‌ها، آب، برق ومؤسسه‌های عمومی نظیر مدارس، دفاتر پستی و زندان‌ها اشاره می‌کند در حکم اجرایی حمایت از زیربناهای حیاتی در سال۲۰۰۱ که توسط رئیس جمهور وقت آمریکا منتشر شده است، زیرساخت‌های حیاتی به تجهیزات، امکانات و خدمات تولید، تبدیل و توزیع برق، مخابرات و ارتباط‌ها از راه دور؛ تجهیزات و امکانات تولید، استفاده، ذخیره و انهدام مواد و انرژی هسته‌ای؛ سیستم‌های اطلاعات دولتی و خصوصی؛ حمل‌و نقل اعم از: راه‌آهن، بزرگ‌راه‌ها، بنادر و راه‌های آبی، فرودگاه‌ها و هواپیماها؛ دام، کشاورزی و سیستم‌های تهیه آب و غذا برای استفاده و مصرف انسان گفته شده است (عبداله خانی، ۲۵۸:۱۳۸۹-۲۵۷).

حفظ زیرساخت‌های ملی

در اهمیت حفظ زیر ساخت‌های ملی باراک اوباما رئیس جمهورآمریکا ۲۹ ماه مه ۲۰۰۹بیان داشت:

زیرساخت‌های دیجیتال به طورفزاینده‌ای به ستون اصلی اقتصادهای شکوفا، جوامع پژوهشی قدرتمند، ارتش‌های قوی، حکومت‌های شفاف و جوامع آزاد تبدیل شده‌اند. فناوری اطلاعات موجب تقویت گفتگوهای فراملی شده و جریان جهانی جابجایی کالا

1 Advanced research projects agency
2 Google
3 Cirital Infrastructure
4 The American Heritage Dictionary

و خدمات را تسهیل کرده است. این پیوندهای تجاری و اجتماعی به بخش جدایی ناپذیر زندگی روزمره ما تبدیل شده‌اند. تمام زیرساخت‌های حیاتی مورد نیاز استمرار زندگی از جمله انتقال آب و برق،کنترل ترافیک هوایی و پشتیبانی از نظام مالی همگی بر سامانه‌های اطلاعاتی شبکه‌ای وابسته هستند.حکومت‌ها هم اکنون می‌توانند از طریق طرح‌های ابتکاری دولت الکترونیکی به کارآمد ساختن شرایط خدمات ضروری بپردازند. جنبش‌های سیاسی و اجتماعی نیز می‌توانند برای ایجاد اشکال جدید وگسترده به اینترنت اتکا کنند، دامنه دسترسی به فناوری شبکه‌ای، جهانی و فراگیر است. برای تمام ملت‌ها زیر ساخت‌های اساسی دیجیتالی یک دارایی ملی محسوب می‌شود و یا اینکه به زودی به دارایی ملی تبدیل خواهد شد. تضمین جریان آزاد اطلاعات، تأمین امنیت و محرمانه ماندن داده‌ها و انسجام شبکه-های در هم تنیده برای پیشرفت اقتصاد آمریکا و جهان، امنیت و ارتقای حقوق جهانی کاملاً ضروری هستند. جامعه جهانی باید به طور یک پارچه و هماهنگ چالش‌های به وجود آمده در نتیجه ورود کنشگران بدخواه به فضای مجازی را شناسایی کند و متناسب با این چالش‌ها سیاست‌های مالی و بین‌المللی را به روز کرده و تقویت کند. اقدامات انجام شده در فضای سایبری دارای پیامدهایی برای زندگی ما در فضای فیزیکی است و ما باید به سمت ایجاد حکومت قانون حرکت کنیم و از خطر احتمال چربش معایب آن بر محاسن آن جلوگیری کنیم. آینده فضای سایبری امن، مطمئن، و شفاف به نحوه شناسایی مناسب این فضا و محافظت از آن از سوی ملت‌ها بستگی دارد. در عین حال باید با کسانی نیز که در صدد بی ثبات کردن یا تضعیف جهان هستند مقابله کنیم، جهانی که به طور فزاینده‌ای به سمت شبکه‌ای شدن در حال حرکت است (کاخ سفید، ۲۰۱۱: ۳).

برخی زیرساخت‌های حیاتی در شیوه زندگی آمریکایی‌ها بسیار حائز اهمیت است که حمایت از این زیرساخت‌ها مستلزم دخالت و فعالیت دولت آمریکا است. در اینجا به یک رهبری دولتی سنجیده همچون سایر حوزه‌ها یعنی جایی که رفاه زندگی آمریکایی در خطر است، نیاز است. این نهادها با همکاری کمپانی‌های گروه‌های صنعتی و آژانس‌های دولتی آمریکا که زیرساخت‌های بنیادی آمریکا را مدیریت می‌کنند، در مقابل حملات سایبری اعلام آمادگی کرده‌اند، اما سعی و تلاش‌های آنها ناکافی بوده و پیشرفت در بخش‌ها و کمپانی‌ها در نوسان و متفاوت بوده است. بر اساس این گزارش، کمپانی‌ها برای فعالیت اقتصادی در حوزه امنیت سایبری با یکدیگر رقابت می‌کنند، زیرا کنترل تهدیدات بسیار مشکل و بازگشت سرمایه‌گذاری مبهم است. اگر کمپانی‌ها در زمینه دفاع علیه حملات سایبری که اکنون در آمریکا بسیار رایج است شکست بخورند، آثار و پیامدهای جبران ناپذیری بر اقتصاد دولت و مردم آمریکا در پی‌خواهد داشت (لرد و شارپ، ۲۰۱۱: ۴۷).

کشور آمریکا به شدت به سیستم‌های رایانه‌ای وابسته است. حوادث ۱۱ سپتامبر به‌طور خاصی به افزایش آگاهی از آسیب‌پذیری‌ها و مسئله فوریت در پاسخگویی تخریب یا اختلال در زیرساخت‌های حساس منجر شد، هم‌چنین دولت تدابیر امنیتی در اینترنت را تشدید کرد. جورج بوش، رئیس جمهور وقت آمریکا، دستور داد ۱/۵ میلیارد دلار بر بودجه تدابیر امنیتی شبکه‌های رایانه‌ای و اینترنت و همچنین

آموزش متخصصانی که با حملات اینترنتی احتمالی تروریست‌ها مقابله می‌کنند، افزوده شود (ضیایی‌پرور، ۱۱۴:۱۳۸۹).

حملات ۱۱ سپتامبر، مسلم ساخت که مسأله حفاظت از زیرساخت‌های حساس به هسته اصلی امنیت ملی تبدیل شده است؛ و این در حالی بود که دولت کلینتون تهدیدات سایبری را یکی از خطرات عمده قرن بیست و یکم تعریف می‌کرد. دولت بوش با چرخش از یک تمرکز بسیار قوی بر ابزارهای سایبری و روش‌های شکل‌گیری تهدید سایبری به سمت ادغام با دیدگاه‌هایی در باب تروریسم پیش رفت. جنبه‌هایی از جنگ اطلاعات و توانایی غلبه کردن در حوزه اطلاعات بار دیگر تبدیل به موضوعات کلیدی امنیت در دستور کارهای سیاسی شد. تهدیدات سایبری در ارتباط مستقیم با بحث حفاظت از زیرساخت‌های حساس است (دان کاولتی، ۱۲۶:۱۳۸۹).

برخی زیرساخت‌های حیاتی از جمله حوزه مسایل مالی، بخش برق و شبکه‌های ارتباطاتی به طور فزاینده‌ای در برابر حملات سایبری آسیب‌پذیر هستند. بخش خصوصی در ایالات متحده در حدود ۸۵ تا ۹۰ درصد زیرساخت‌های حیاتی این کشور را در اختیار دارد و فعالان این بخش‌ها برای کنترل و اداره این فرایندهای حساس از فضای سایبری استفاده می‌کنند. به عنوان مثال، تنظیم سطح کلر در آب، باز و بسته کردن شیرها و دریچه‌ها، کنترل جریان نفت و انجام معاملات مالی از جمله این موارد به شمار می‌آیند. وقوع یک حمله سایبری و بروز اختلال در این شبکه‌ها حتی برای مدت زمان اندکی می‌تواند موجب از بین رفتن اموال، منابع و کشته شدن انسان‌های بی‌گناه شود (واتیز، ۲۰۰۲: ۲).

آمریکا به هنگام حفاظت از زیرساخت‌های بنیادی نباید بسیار خام و بیش از حد مقرراتی عمل کند. آمریکا باید از راه‌حل‌های بازار تا حد ممکن جانبداری کند. این هدف فراگیر باید تأمین کنندگان زیرساخت‌های بنیادی و پیشرفته را قادر سازد تا از امنیت بیشتری نسبت به مجموعه گسترده‌ای از تهدیدات برخوردار باشند، در حالی که برای تأمین کنندگان کمتر توسعه یافته این امکان را فراهم می‌سازد تا به سطح بالایی از امنیت دست یابند. برای دستیابی به اهداف فوق و برای دفاع از زیرساخت‌های ملی، دولت ایالات متحده گام‌های متعددی برداشته است. اگرچه پرداختن به تمام آن گام‌ها از دامنه این مطلب خارج است اماچند مورد، ارزش مطرح شدن دارد (لرد و شارپ، ۲۰۱۱: ۴۷).

گام اول، تأسیس یک مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای[1] در دانشگاه کارنگی- ملون است. این مرکز، در سال ۱۹۸۸ پس از آنکه یک رویداد مهم در اینترنت، هزاران رایانه را دستخوش اختلال کرد تأسیس شد. اداره پروژه‌های پیشرفته وزارت دفاع که اینترنت را بنا نهاد، مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای را طوری بنیان نهاده که ایالات متحده برای رویدادهای آتی بهتر آماده باشد. مرکز فوق دارای یک نقطه تماس۲۴ ساعته و یک نقطه مرکزی برای مشخص کردن آسیب پذیری‌ها و رفع آنها به کمک فروشنده است (عبداله خانی، ۴۰:۱۳۸۹).

گام دوم، تشکیل کمیسیون ریاست جمهوری درباره حفاظت زیرساخت‌های اساسی[2] در ژوئیه ۱۹۹۶ است. از این کمیسیون خواسته شد آن گروه از

1 CERT/CC
2 PCCIP

زیرساخت‌های حساس کـه سیسـتم‌هـای حمایـت از جـان را تشـکیل مـی‌دهنـد، مطالعـه کننـد و آسـیب پـذیری‌هـای آنهـا را در برابـر گسـتره‌ی وسـیعی از تهدیدها مشخص نمایند و برای محافظـت از آنهـا در آینده، راهبردی پیشنهاد کنند. سال‌های ۱۹۹۷ و ۱۹۹۸ در واقع سال‌های آستانه ارایه دیدگاه‌های مختلـف در باب تهدیدهای سایبری بوده است. فضـای تخصـیص داده شده به موضوع‌های مربوط به تهدیدهای سایبری در راهبردهای امنیت ملـی ایـالات متحـده آمریکـا در همین زمان مشابه رشد باورنکردنی پیدا مـی‌کنـد، بـه علاوه تهدیدهای سایبری بـه مثابـه یکـی از خطـرات ترجیحی برای پاسخگویی در میان تهدیدهای «جدید» جـای خاصـی پیـدا مـی‌کنـد. در گـزارش کمیسـیون ریاست جمهـوری دربـاره حفاظـت زیرسـاخت‌هـای اساسی تهدیدهای سایبری، حتی از تهدیدهای جدیـد نیز خطرناک‌تـر توصـیف شـده بودنـد (دان کـاولتی، ۱۲۶:۱۳۸۹).

گام سوم،کنگره باید در قانون امنیت داخلـی سـال ۲۰۰۲ تجدید نظـر کنـد تـا وزارت امنیـت داخلـی از اختیارات بیشتری در حفـظ زیرسـاخت‌هـای بنیـادی آمریکا در فضای سایبری برخوردار شود. این موضوع باید اختیار در مورد قواعد موضوعی تحت صـلاحیت را شـامل شـود کـه بـر اسـاس آن تهیـه‌کننـدگان زیرسـاخت‌هـای بنیـادی، مبنـای محکمـی را بـرای اقدامات امنیتـی مـی‌پذیرنـد. اگرچـه رئـیس جمهـور اختیارات فوق را از طریق دستورالعمل‌های مشخصـی ارایه کرده است، امـا ایـن اختیـارات بایـد بـر اسـاس قـانون مـدون شـود تـا در نهایـت بـه تقویـت امـر پاسخگویی منتهی شود، هـم چنـین کنگـره بـا وضـع قوانین سـایبری بایـد زمینـه را بـرای اسـتراتژی‌هـای نظارتی دقیق فـراهم کنـد کـه بـا اهـداف و نیازهـای بخش‌هـای خـاص متناسـب باشـد. زیرسـاخت‌هـای بنیادی آمریکا یکپارچه نبـوده و قواعـد ارتباطـات راه دور (مخـابرات) بایـد بـا حفـظ حـریم خصوصـی و ناشناخته ماندن بر اساس ارزش‌های محـوری آمریکـا طراحی شود و این قواعد باید از قواعد شبکه برقـی- که حریم خصوصی در آن به عنـوان دغدغـه حسـاب نمی‌شود- متفاوت باشد (لرد و شارپ، ۲۰۱۱: ۴۸).

به رغم تلاش‌های فراوان دولت آمریکـا و بخـش خصوصی برای تقویت امنیت سایبری، این تهدیدهای سایبری فزاینده و پیچیـده در حـال پیشـرفت و رشـد است و نیازمند راه حل‌هایی فـوری و اساسـی اسـت. حال این سوال مطرح است که آیا آمریکا در برابر این چالش به پا خواهد خواست؟ با توجه به پژوهش‌های فراوان و مذاکره زیاد با افراد حاضر در دولت، بخـش نظامی، بخش خصوصی و سازمان‌هـای غیـر دولتـی، جواب خوشبی نانه به ایـن پاسـخ، آری اسـت. البتـه موفقیت در این امر نیازمند مدیریتی قوی‌تر و فعال‌تـر از سوی دولت آمریکا است. دولـت بـه شـرکت‌هـا و پژوهشـگرانی نیـاز دارد کـه سـریع‌تـر از مجرمـان و جاسوسان دسـت بـه نـوآوری بزنـد. عـلاوه بـر ایـن نیازمند افراد و شرکت‌هایی در سرتاسر آمریکا و دنیـا است که مسئولیت امنیـت خـود در ایـن زمینـه را بـر عهده بگیرند. نباید منتظر یک فاجعه دیجیتالی بـود تـا آن‌گاه به فکر تغییر روند عـدم امنیـت سـایبری افتـاد (لرد و شارپ، ۲۰۱۱: ۷).

تهدیدهای سایبری و ایالات متحده آمریکا

مـا بـه‌طـور فزاینـده‌ای در معـرض خطـر قـرار داریم.آمریکا به رایانه‌ها وابسـته اسـت... . تروریسـت فردا شاید قادر به ایجاد تخریب‌های وسیع‌تری توسط

صفحه کلید باشد تا یک بمب. ملت ما هم‌اکنون در معرض خطر جدی حملات سایبری است که می‌تواند به روح و اقتصاد ما به مراتب بیش از حملات یازده سپتامبر آسیب جدی وارد کند. (اظهارات ریچارد کلارک مشاور سابق کاخ سفید و بیش از ۸۰ دانشمند علوم رایانه‌ای در نامه‌ای به بوش) (دان کاولتی، ۱۳۸۹:۱).

در جوامع پیشرفته مانند آمریکا که به شبکه‌های الکترونیکی متکی هستند، آسیب پذیری در برابر حملات تروریستی، سرقت و خرابکاری در سطح ملی مطرح است. بنابراین، تأکید زیادی بر تروریسم اطلاعاتی و جنگ سایبرنتیک صورت می‌گیرد. به گونه‌ای که «حتی یک مقام امنیتی آمریکا گفته است که با یک میلیارد دلار و بیست نفر متخصص خبره رایانه می‌تواند کل آمریکا را فلج کند، یک تروریست نیز می‌تواند به این توانایی دست یابد». از این رو، تأثیر حمله به شبکه‌های رایانه‌ای از تأثیر حملات شیمیایی و میکروبی بیشتر است (رایش، ۱۳۸۱:۵۵).

تلاش‌های ایالات متحده مانند استراتژی ملی برای فضای مجازی امن از سال ۱۹۹۸ تا ۲۰۰۳ و طرح جامع امنیت سایبری در سال ۲۰۰۸ و طرح‌هایی دیگری که در این زمینه به منصه ظهور رسانده است، نشان دهنده اهمیت این حوزه و به طور اخص خطراتی که در این حوزه امنیت ملی آمریکا را تهدید می‌کند، است. همان‌طورکه بیان کردیم؛ سال‌ها است که دولت آمریکا در اسناد امنیت ملی خود بر خطر فراوان تهدیدهای سایبری و ارتباط تنگاتنگ آنها با جرم، جاسوسی و جنگ تأکید می‌کند. این تهدیدها به چالشی جدی برای ایالات متحده تبدیل شده‌اند. کاخ سفید در ماه می ۲۰۱۱ راهبرد بین‌المللی خود در فضای سایبری را منتشر کرد که در آن چارچوبی واحد برای موضوعات متعدد امنیت سایبری در نظر گرفته است. امنیت سایبری معضلی چند بعدی است «تهدیدهی امنیت سایبری یکی ازجدی‌ترین چالش‌های امنیت ملی،ایمنی عمومی واقتصادی ملت ما است. فناوری‌هایی که موجب رهبری وبرتری می‌شوند درعین حال موجب تقویت موضوع‌هایی می‌شوند که موجبات تخریب و نابودی را فراهم می‌آورند» (کاخ سفید، ۲۰۱۰: ۴۵).

حملات سایبری[1]

حمله سایبری چیزی متفاوت از جنگ سایبری است. حمله سایبری اختلال در صحت یا درستی داده‌ها است که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که به خروجی-های اشتباه منجر می‌شود، صورت می‌گیرد (ردریگز، ۲۰۰۶: ۹ و ۱۰).

حملات سایبری شامل چهار حوزه می‌شود:

۱- از دست دادن کلیت داده‌ها ۲- از دست دادن قابلیت ۳- از دست دادن اطلاعات محرمانه ۴- و تخریب فیزیکی (ارمی، ۲۰۰۵: ۱ تا ۳).

برای مثال آب، برق، بانکداری، 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 یک حمله اینترنتی می‌تواند همانند بازی دومینو در آنها اختلال ایجاد کند، اختلال در یک سیستم مساوی با اختلال در سیستم‌های دیگر است و ادامه این روند از تاثیرهای بالقوه حملات اینترنتی است (اسلام و همکاران، ۲۰۱۱: ۵ و ۶).

1 Cyber Attacks

در تعریف جنگ سایبری باید گفته شود که تعریف آن از لحاظ تئوری بسیار آسان‌تر از تعریف آن به صورت عملی است زیرا تاکنون هیچ جنگ سایبری به وقوع نپیوسته است. اگرچه جنگ سایبری می‌تواند تأثیرات مخربی داشته باشد اما در آن از ویرانی و خونریزی‌های مرسوم در جنگ واقعی خبری نیست. اگرچه اطلاعات موجود در جنگ سایبری مستقیماً عامل مرگ انسانی نمی‌شود اما این اطلاعات ممکن است سیستم‌ها و برنامه‌هایی را از بین ببرد که جان انسان‌ها را به خطر بیندازد . حملات سایبری ممکن است خطرات مشخصی به وجود آورد اما تا رسیدن به مرحله جنگ سایبری، فاصله زیادی دارد زیرا هدفی که مورد حمله قرار می‌گیرد توانایی و علاقه واکنش و حمله متقابل را ندارد (لرد و شارپ، ۲۰۱۱: ۱۹).

با ذکرچند مثال بزرگی خطرات نهفته در حملات سایبری را در ایالات متحده و علیه این کشور مورد بررسی قرار می‌دهیم.

شخصی در سال ۲۰۰۹، چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه‌جنگنده‌های مشترک ۳۰۰ میلیارد دلاری پنتاگون را به سرقت برد. علاوه بر این، بیشتر مجرمان اینترنتی از مجازات فرار کرده‌اند. بدیهی است که این فعالیت پرسود و اغلب بدون مجازات، در واقع تهدیدی برای امنیت ملی است (پریتز و اسچریست، ۲۰۱۰: ۱۴).

در مبارزات انتخابات ریاست جمهوری ۲۰۰۸، شبکه‌های کامپیوتری باراک اوباما و جان مک کین مورد حمله قرار گرفت که هدف از آنهایی بردن به برنامه‌های آتی نامزدهای انتخاباتی بود (لرد و شارپ، ۲۰۱۱: ۱۷).

هک کردن سازمان سیا، اف بی آی، برای ارعاب یا اجبار مردم آمریکا مثال دیگر هک کردن پایگاه داده‌های بیمارستان و تغییر اطلاعات بیمار است که باعث مصرف نادرست دارو می‌شود. در ۲۰۰۳ طرح تجارت الکترونیک دلار اعلام کرد برای یک سال اگر اینترنت هک یا دستکاری شود در ۶,۵ میلیون دلار معاملات جهانی اختلال بوجود می‌آید (پلاندا، ۲۰۰۵: ۳).

چند تن از مجرمان اخیراً محکوم شده‌اند، که از مهارت‌های خود برای جرایم اینترنتی و بدست‌آوردن اطلاعات کارت‌های اعتباری به سرقت رفته برای تأمین منابع مالی فعالیت‌های تروریستی‌شان استفاده کرده‌اند. امکان دارد که جنایت‌کاران و گروه‌های تروریستی تلاش کنند راه‌هایی برای همکاری با یکدیگر و نوع جدیدی از تهدید را بوجود آورند، که در آن افراط‌گرایان به ابزارهای قدرتمند برای جرایم اینترنتی و سرقت اطلاعات شخصی و یا منحل‌کردن سیستم‌های کامپیوتری، دسترسی پیدا کنند (نگره و وارد، ۲۰۰۸: ۸).

مثال معروف حمله‌ی هکرها مربوط به سال ۱۹۹۸ است که سه پسر ۱۶،۱۷،۱۸ساله با نام‌های مستعار ماکیاول، قدکوتاه، تحلیلگر، برنامه‌ریزی شده‌ترین حمله علیه زیرساخت‌های نظامی آمریکا در فضای سایبر را انجام دادند. اگرچه انگیزه‌ی این افراد سیاسی یا نظامی نبود ولی آنها توانستند به شبکه‌های پنتاگون، دانشگاه برکلی، دانشگاه MIT و کتابخانه‌های ملی نفوذ کنند (حسن‌بیگی، ۱۳۸۴: ۱۶۰).

در ۱۹۸۸، کرم موریس آرپانت را که در واقع اینترنت ابتدایی بود، دچار توقف کرد. واقعه

کاکوزاگ[1] در واقع دزدی رایانه‌ای بود که یک هکر آلمانی تلاش کرده بود به شبکه‌های رایانه‌ای ایالات متحده آمریکا به ویژه در ارتباط با امنیت ملی این کشور دسترسی پیدا کند. در اوایل دهه ۱۹۸۰، ما شاهد افزایش و رشد آگاهی درباره حضور و نفوذ جاسوسان خارجی برای کشف راه‌های جدید کسب اطلاعات عالی طبقه‌بندی شده هستیم (دان کاولتی، ۲:۱۳۸۹).

ویروس کامپیوتری با نام استاکس نت که به سانتریفیوژهای هسته‌ای ایران فرستاده شد، توانست با روش‌های مختلف آنها را از کار بیندازد. طبق گزارش رسانه‌های مختلف، این اتفاق نمونه‌ای مشخص از یک حمله سایبری با تأثیری محرک بود. این ویروس پیشرفته که در ظاهر با هدف حمله به سامانه‌های صنعتی ایران طراحی شده بود به دلیل تکنیک‌های ویژه تکثیری آن بیش از صد هزار سامانه در ۱۵۵ کشور جهان را آلوده کرد. در واقع، این آلودگی‌های اضافی خسارات جانبی محسوب می‌شوند زیرا این حوادث تأثیرات جانبی ناخواسته ویروس استاکس‌نت محسوب می‌شد (لرد و شارپ، ۲۰۱۱: ۱۳).

اما شاید جالب‌ترین مثال به کرم رایانه‌ای نیمدا[2]مربوط می‌شود که به دلیل تاثیرگذاری مخرب بالای آن و هم‌چنین برخورداری از قابلیت‌های دیگر، مانند ویروس تروجان[3] به کرم چهار سر[4] معروف شده بود. این کرم رایانه‌ای یک هفته پس از واقعه یازده سپتامبر ۲۰۰۱، منتشر شد و خسارات زیادی به ویژه به سیستم‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد(کدخدایی و ساعد، ۱۳۹۰: ۹۳).

بنابراین، چالش امنیت سایبری و تهدیدهای آن هم مهم و هم پیچیده است. دستیابی به ترتیب‌های مؤثر حکومت در این حوزه، به یک استراتژی جامع که شامل اقدامات هماهنگ بوسیله حکومت، بخش خصوصی و شهروندان نیاز دارد. جامعه جهانی نیز به صورت واضح، منافع مشترکی در حمایت امنیت سیستم‌های سایبری همکاری و اقدام فوری نیازمند است (چرتوف، ۲۰۰۸: ۴۸۴).

در راستای چنین اهمیتی بود که در ۲۹ می سال ۲۰۰۹، رئیس جمهور آمریکا اعلام کرد که فضای سایبری به عنوان یک دارایی مهم ملی است که ایالات متحده با تمام معنی از آن دفاع می‌کند (لویس، ۲۰۱۱: ۳).

تلاش‌های دولت آمریکا برای ارتقای امنیت سایبری

آمریکایی‌ها به دلیل وابستگی زیرساخت‌های حیاتی کشورشان به اینترنت برای دولت نقش برجسته‌ای قائلند و هدایت امنیت ملی در فضای سایبر را وظیفه‌ی دولت می‌دانند.آنها بر همکاری و مشارکت بخش‌های خصوصی و دولتی تأکید داشته و این همکاری را از نوع اشتراک اطلاعات، امکانات و آموزش می‌دانند و دولت مرکزی را نیز به عنوان هماهنگ کننده‌ی اصلی در نظر گرفته‌اند.

اولویت‌های اساسی امنیت فضای سایبر عبارتند از:

۱) سیستم پاسخگویی امنیت فضای سایبر ملی؛

۲) برنامه کاهش آسیب‌پذیری و تهدید امنیت فضای سایبرملی؛

۳) برنامه آموزش و اطلاع‌رسانی امنیت فضای سایبر ملی؛

1 Cukoo`s egg
2 Nimda
3 Trojan virus
4 Four Headed worm

۴) تأمین فضای سایبر دولتی؛
۵) همکاری بین‌المللی.

اولویت اول در مورد ارایه واکنش لازم به حوادث سایبر به منظور کاهش خسارات احتمالی است. اولویت‌های دوم، سوم، چهارم آسیب‌پذیری و خطر تهدید حملات سایبری راکاهش می‌دهند و اولویت پنجم نیز برای اجتناب از حملات سایبر خارجی که بر امنیت ملی تأثیر داشته و همچنین برای بهبود مدیریت بین‌المللی و پاسخگویی به چنین حملاتی در نظر گرفته شده است (حسن بیگی، ۱۳۸۴:۲۶۳-۲۶۲).

در ژانویه سال ۲۰۰۸، دولت بوش طرح جامع امنیت سایبری ملی[1] در جهت تلاش برای امن‌تر ساختن ایالات متحده در مقابل تهدیدهای سایبری را آغاز کرد. این طرح جامع، ایجاد سیاست، استراتژی و راهنمایی‌هایی برای سیستم‌های امنیتی فدرال بود. همچنین رویکردی است که تهدیدهای آینده اینترنتی و فناوری و نیازهای دولت فدرال به ادغام بسیاری از توانایی‌های فنی و سازمانی آن را برای پاسخ بهتر به تهدیدهای پیچیده را پیش‌بینی می‌کند (تئوهری و رولینز، ۲۰۰۹: ۳).

در سال ۲۰۰۹ دولت اوباما، مجموعه‌ای از یک استراتژی برای امنیت سایبری به منظور مقابله با تهدیدهای تدوین و صورت‌بندی کرد. این ابتکار دوازده دستورالعمل نظامی، غیرنظامی، شبکه‌های دولتی و سیستم‌های زیرساخت را پوشش می‌دهد. در قدم نخست تأکید رئیس جمهور به کار هماهنگ بخش خصوصی، جامعه پژوهشی و شهروندان برای ایجاد زیرساخت‌های اینترنتی قابل اعتماد و انعطاف‌پذیر که از مزیت نسبی آمریکا و پیشرفت‌های ملی و امنیت میهنی محافظت کند (استون، ۲۰۱۰: ۶).

دولت اوباما با بهره‌گیری از اقدامات دولت‌های بوش و کلینتون تأکید فراوانی بر جدی بودن تهدیدهای سایبری داشته و با جدیت هر چه تمامتر درصدد تقویت امنیت سایبری آمریکا است. اجرای برنامه‌هایی با عنوان «مرور سیاست فضای سایبری»، ایجاد فرماندهی سایبری آمریکا، ارتقای نقش وزارت امنیت داخلی، افزایش بودجه برنامه‌های کلیدی و تدوین راهبرد ملی هویت‌های مورد اعتماد در فضای سایبری و اتخاذ راهبرد بین‌المللی در فضای سایبری از جمله مهم‌ترین دستاوردهای دولت اوباما در فضای سایبری محسوب می‌شود. دولت اوباما هم‌چنین فردی را به عنوان مسئول هماهنگ‌کننده امنیت سایبری در کاخ سفید منصوب کرده است که دسترسی دائم به رئیس‌جمهور دارد و با گروه‌های امنیت ملی و اقتصادی همکاری نزدیکی دارد. فرماندهی سایبر ایالات متحده آمریکا موسوم به «سایبرکام»[2] در ۲۳ ژوئن ۲۰۰۹ تصویب شد و ۱۱ ماه پس از آن تاریخ به مرحله‌ای رسید که پنتاگون آن را قابلیت اولیه انجام عملیات می‌نامد. رازوف با تأکید بر آنکه سایبرکام تا پایان سال ۲۰۱۰ بطور کامل عملیاتی می‌شود افزود: مقر فرماندهی سایبر آمریکا در شهر "فورت مید" ایالت مریلند؛ یعنی جایی که «آژانس امنیت ملی» آمریکا نیز در آن واقع شده است، قرار دارد (گورمن، ۲۰۰۹).

امنیت سایبری برای حمایت و پیشبرد منافع ملی آمریکا امری مهم و حیاتی است. همانگونه که در راهکار امنیت ملی سال ۲۰۱۰ آمریکا بیان شد، این

1 CNCI

2 cybercom

منافع عبارتند از:

– امنیت آمریکا، شهروندان، دوستان و شرکای آن

– اقتصاد رو به رشد آمریکا در سیستم اقتصادی بین‌المللی که رفاه و فرصت‌ها را ارتقا می‌بخشد

– احترام به ارزش‌ها جهانی در کشور و در سرتاسر دنیا

توانایی آمریکا برای رسیدن به این منافع به میزان بسیار زیادی بستگی به دسترسی امن و قابل اعتماد به اینترنت دارد که هیلاری کلینتون، وزیر امور خارجه آمریکا آن را اینگونه تعریف کرد: مجموعه‌ای که قدرت و پتانسیل دیگر افراد را تقویت می‌کند. در صورت وجود اعتماد در فضای اینترنت، امنیت سیستم‌های مرتبط با آن و اعتماد به استفاده‌کنندگان، توانایی آمریکا برای دسترسی به این منافع افزایش خواهد یافت (لرد و شارپ، ۲۰۱۱: ۱۲).

نهادهای ایالات متحده و تهدیدهای سایبری

حوزه امنیت سایبری به اندازه‌ای پیچیده است که نمی‌توان آن را صرفاً با یک سازمان یا مرکز مدیریت کرد. امنیت سایبری دارای ابعاد گسترده‌ای است و افراد زیادی در آن حضور دارند. در این بخش نقاط ضعف و قدرت برخی سازمان‌ها و نهادهای کلیدی دولت آمریکا مورد تحلیل قرار خواهد گرفت.

۱. کاخ سفید

کاخ سفید توجه فراوانی به موضوع امنیت سایبری از خود نشان داده است. کاخ‌سفید در آوریل سال ۲۰۱۱ راهبرد ملی هویت‌های مورد اعتماد در فضای سایبری را منتشر کرد که دولت از آن به عنوان یک «اکوسیستم هویت» بر خط نام می‌برد. اکوسیستم هویت نام دیگر طرح اعتماد هویت است که به هر یک از شهروندان آمریکایی در صورت تمایل، یک شناسه معتبر و تأئید شده اختصاص می‌دهد که می‌توانند در تراکنش‌های اینترنتی از آن استفاده کنند. این راهبرد خواستار شکل‌گیری نهادها و موجودیت‌های قابل اعتماد به ویژه در بخش خصوصی است تا از این طریق بتوان سامانه‌ای برای احراز هویت‌های دیجیتالی امن به وجود آورد. به رغم تمام این پیشرفت‌ها، کاخ سفید هنوز هم با مشکلات جدی در حوزه مدیریت، رهبری و هماهنگی در حوزه امنیت سایبری مواجه است. امنیت سایبری معضلی چند بعدی است، حجم کارها بسیار بالاست و تعداد کارمندان کاخ سفید نیز برای انجام چنین وظیفه بزرگی، بسیار کوچک است (لرد و شارپ، ۲۰۱۱: ۳۱).

۲.وزارت دفاع

وزارت دفاع فضای سایبری را در کنار زمین، دریا، هوا و جو بیرونی به عنوان پنجمین عرصه جنگ قرار داده است. این وزارتخانه مرکزی را با عنوان فرماندهی سایبری تشکیل داده است که تحت مدیریت فرماندهی راهبردی فعالیت می‌کند. هدف از تشکیل این فرماندهی حمایت از شبکه‌های نظامی ایالات متحده است. وظیفه فرماندهی سایبری، متمرکز ساختن تلاش‌های صورت گرفته در حوزه امنیت سایبری در ارتش ایالات متحده است. تمام بخش‌های ارتش ایالات متحده درصدد برنامه‌ریزی مجدد عملیات‌های سایبری خود هستند و در فرماندهی سایبری ادغام خواهند شد. «نیروی هوایی بیست و چهارم» که در آگوست سال ۲۰۰۹ تشکیل شد سازمانی جنگی است که مسئولیت ایجاد، راه‌اندازی و دفاع از شبکه‌های نیروی هوایی را بر عهده دارد و تمام عملیات‌های انجام شده در فضای

سایبری را مدیریت می‌کند. نیروی هوایی در سال ۲۰۱۰ دکترین بنیادین خود در فضای سایبری را منتشر کرد. در ژانویه همان سال، نیروی دریایی فرماندهی سایبر ناوگان ایالات متحده را تشکیل داد و از ناوگان دهم خواست تا کنترل عملیاتی نیروهای سایبری نیروی دریایی را در اختیار خود بگیرد و عملیات‌های فضای سایبری را مدیریت کند. در همان ماه نیز نیروی دریایی با هدف هماهنگی فعالیت‌های خود در فضای سایبری اقدام به تشکیل فرماندهی سایبری نیروهای دریایی کرد (کاخ سفید، ۲۰۱۱: ۸ و ۹).

جدول (۱) بودجه درخواستی وزارت دفاع در حوزه امنیت سایبری برای سال مالی ۲۰۱۲

بودجه درخواستی وزارت دفاع در حوزه امنیت سایبری برای سال مالی ۲۰۱۲ (به میلیون دلار)	
ارتش	۴۳۲
نیروی دریایی	۳۴۷
نیروی هوایی	۴۴۰
مراکز دفاعی	۱۶۰۰
سایر بخش‌ها (از جمله فرماندهی سایبری)	۴۴۳
مجموع	۳۲۶۲

(لرد و شارپ، ۲۰۱۱: ۳۵).

۳.آژانس امنیت ملی

آژانس امنیت ملی آمریکا زیر نظر وزارت دفاع ایالات متحده آمریکا اداره می‌شود. این سازمان در سال ۱۹۵۲ تأسیس شد و بالغ بر ۱۰۰ هزار نفر پرسنل دارد. این افراد در آمریکا و ایستگاه‌های شنود مستقر در خارج مشغول به فعالیت هستند. وظیفه اصلی این نهاد امنیتی نظارت بر مخابرات و فعالیت های ماهواره ای و کشف رمز در ایالات متحده آمریکا و سایر نقاط دنیا است. بی‌شک ارتباط‌های افراد بر روی شبکه اینترنت نیز تحت کنترل شدید این آژانس قرار دارد. این آژانس از اعضای کلیدی جامعه اطلاعاتی ایالات متحده آمریکا بوده و از محرمانه‌ترین سازمان‌های جاسوسی در جهان به شمار می‌رود. باید گفت کارکرد اصلی و عمده آژانس امنیت ملی آمریکا تأمین اشراف اطلاعاتی است. اشراف اطلاعاتی توسط این نهاد از طریق رصد کاربران در فضای مجازی و بطور مشخص در فضای اینترنت رقم می‌خورد (دان کاولتی، ۱۳۸۹:۸۰).

گستره جهانی این آژانس تا حدودی ناشی از مشارکت آن در طرح اشلون[1] است. این طرح یک سیستم نظارت جهانی، تحت اداره ۵ کشور متشکل از آمریکا، انگلستان، کانادا، استرالیا و نیوزیلند است. سیستم جاسوسی اشلون از ۱۲۰ ماهواره ارتباطاتی، اکتشافی و نظارتی تشکیل شده که در مدارهای ثابتی دور زمین می‌گردند. علاوه بر این ماهواره‌ها، تعداد بسیار زیادی گیرنده‌های زمینی، در نقاط مختلف دنیا نصب شده تا نقاط کور ماهواره‌ها را پوشش دهند.این ماهواره‌ها و گیرنده‌ها وظیفه دارند، روزانه حدود سه میلیارد تماس تلفنی، فاکس و ایمیل را ذخیره کرده،

1 Echelon

به رایانه‌های مادری که در این پنج کشور وجود دارند، انتقال دهند. این اطلاعات پس از ترجمه خودکار به زبان انگلیسی، تحت یک پردازش محتوایی دقیق قرار می‌گیرد (ضیایی پرور، ۱۳۸۹:۱۴۶). هر چند پروژه آمریکا در راه‌اندازی اشلون نتوانست جلو حملات یازده سپتامبر را بگیرد ولی هزینه‌ها و بودجه‌های سازمان‌های ذی ربط از قبیل سیستم هوا فضای ملی آمریکا افزایش یافته است و وظایف سیاسی آنها که تعرض بیشتر در حریم خصوصی افراد را در پی دارد، افزون‌تر شده‌اند (هالپین و دیگران، ۴۲۲:۱۳۸۹).

برخی از کارشناسان پیشنهاد داده‌اند که این آژانس باید رهبری فعالیت‌های بخش امنیت سایبری در دولت را بر عهده گیرد. با این حال سایر کارشناسان بر این باورند که ماهیت فوق‌العاده محرمانه این آژانس می‌تواند در نهایت به شفافیت کمتر، اعتماد و مشارکت کمتر منجر شود که خروجی نهایی آن نیز تضعیف امنیت سایبری خواهد بود. دولت اوباما اما در این ارتباط راه‌حل میانه و بینابینی را در پیش گرفته است. بدین معنا، درحالیکه وزارت امنیت داخلی همچنان رهبری و مدیریت محافظت از شبکه‌های سایبری دولت را بر عهده دارد. در عین حال توانمندی‌های پیشرفته آژانس امنیت ملی نیز مورد استفاده قرار می‌گیرد. این رویکرد در یادداشت تفاهمی که میان وزارت دفاع و وزارت امنیت داخلی به امضاء رسید نیز مورد توافق قرار گرفت (لرد و شارپ، ۲۰۱۱: ۳۳).

۴. وزارت امنیت داخلی

مهم‌ترین تغییر در حوزه تهدیدهای سایبری، تأسیس وزارت امنیت داخلی است. استقرار چنین وزارتخانه‌ای مورد حمایت کمیسیون امنیت ملی قرن ۲۱ ایالات متحده قرار گرفته بود. کمیسیونی که با نام کمیسیون هارت-رادمن[1] معروف شده بود. گزارش نهایی کمیسیون در فوریه ۲۰۰۱، کامل شد و احتمال رخداد وقایع راهبردی مثل یازده سپتامبر را محتمل توصیف کرده بود و گفته بود که ایالات متحده بشدت در مقابل وقوع حملات در سرزمین خود آسیب‌پذیر است:

حملات می‌تواند از طریق تسلیحات تخریب همگانی باشد. همانند مرزهای فیزیکی ایالات متحده، مرزهای سایبری نیز بسیار نفوذ پذیر هستند و به تبع، زیرساخت‌های حساس ایالات متحده که اقتصاد این کشور بسیار به آن وابسته است می‌تواند هدف بازیگران غیردولتی و دولتی قرار بگیرد. برتری جهانی کنونی آمریکا ضامن مصونیت آمریکا از چنین خطراتی نیست (دان کاولتی،۱۴۸:۱۳۸۹-۱۴۷).

وزارت امنیت داخلی مسئول اصلی تضمین امنیت شبکه‌های طبقه‌بندی نشده دولت ایالات‌متحده به شمار می‌آید. در گزارش ۴ سالانه وزارت امنیت داخلی که در سال ۲۰۱۰ منتشر شد امنیت سایبری یکی از ۵ حوزه اصلی مأموریت این وزارتخانه محسوب می‌شود. ارایه نظرات کارشناس فنی به بخش خصوصی و سازمان‌های مسئول در زیرساخت‌های حیاتی، ارتقای سطح آگاهی عمومی و یکپارچه و هماهنگ ساختن واکنش‌ها در قبال حوادث مهم از مهمترین اقدامات وزارت امنیت داخلی است. این وزارتخانه هم چنین سازمانی را با عنوان «تیم آماده‌سازی اضطراری رایانه‌ای» مدیریت می‌کند که مسئولیت انجام اقدامات مناسب در قبال حملات سایبری را بر عهده دارد. در نهایت اینکه،

1 Hurt-Rudman

وزارت امنیت داخلی با هدف تبادل اطلاعات و اجرای برنامه‌های مدیریت خطرات امنیت سایبری با بخش خصوصی، دولت‌ها، حکومت‌های محلی و شرکای بین‌المللی همکاری می‌کند(www.dhs.gov)

جدول (۲) بودجه در خواستی وزارت امنیت داخلی در بخش امنیت سایبری برای سال مالی۲۰۱۲

بودجه در خواستی وزارت امنیت داخلی در بخش امنیت سایبری برای سال مالی	
شناسایی و تجزیه و تحلیل	۸۴
هماهنگی و تبادل اطلاعات	۴۸
برنامه های آماده سازی برای کاهش خسارات	۱۹۰
تیم آمادگی اضطراری رایانه ای ایالات متحده	۳۹۱
طراحی ابتکاری راهبردی	۶۵
برنامه‌های کمکی	۷
خدمات ارتباطی اولویت دار	۵۷
برنامه های ارتقای سطح ارتباطات	۱۳
برنامه های حفاظت از زیرساختهای حیاتی	۱۱
شبکه‌های نسل بعد	۲۵
اداره ارتباطات اضطراری	۴۳
مجموع	۹۳۶

(لرد و شارپ، ۲۰۱۱: ۳۵).

اتخاذ یک دستورالعمل بین‌المللی در زمینه امنیت سایبری

ده برنامه کلیدی برای تقویت امنیت سایبری ایالات متحده در سمپوزیومی که در ۲ مارس ۲۰۱۰ از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی ایالات متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، ارایه شده است:

۱) سازمان و رهبری منسجم برای تلاش‌های فدرال برای امنیت سایبری و شناسایی امنیت سایبری به عنوان یک اولویت ملی؛

۲) شفاف‌سازی هر چه بیشتر برای امنیت سایبری بهتر در زیرساخت‌های حیاتی و توسعه راه‌های جدید برای کار با بخش خصوصی؛

۳) سیاست خارجی که تمام ابزار قدرت ایالات متحده برای ایجاد هنجارها، رویکردهای جدید به حکومت و عواقب اقدامات مخرب در فضای مجازی را در بر می‌گیرد. سیاست جدید باید چشم‌اندازی برای آینده اینترنت جهانی روشن کند؛

۴) توانایی گسترش استفاده از هوش و توانایی‌های نظامی برای دفاع در برابر تهدیدهای پیشرفته خارجی؛

۵) نظارت برای تقویت حریم خصوصی و آزادی‌های مدنی، با قوانین و فرآیندهای روشن و سازگار با فناوری‌های دیجیتالی؛

۶) بهبود تشخیص هویت برای زیرساخت‌های حیاتی؛

۷) ایجاد یک نیروی کار گسترده با مهارت کافی امنیت سایبری؛

۸) تغییر سیاست مالکیت برای اداره بازار به سمت امنیت بیشتر تولیدات و خدمات؛

۹) سیاست تجدید نظر شده و چارچوب قانونی برای هدایت اقدامات امنیت سایبری دولت؛

۱۰) پژوهش، توسعه و تمرکز بر روی مشکلات امنیت سایبری و فرآیند برای شناسایی این مشکلات و تخصیص بودجه در یک روش هماهنگ شده است.

دولت آمریکا باید دستورالعمل بین‌المللی خود برای امنیت سایبری را ارتقا بخشد. در کوتاه مدت، دولت باید همکاری بیشتری با شرکای معاهدات آمریکایی داشته باشد تا بدین وسیله تبادل اطلاعات، واکنش مناسب به بحران‌ها و اقدامات نظامی مشترک افزایش پیدا کند. در بلندمدت باید از مجرای قانونی با سهامداران بین‌المللی همکاری داشت تا بتوان به قراردادهایی چند طرفه و مهم دست یافت (CSIS، ۲۰۱۱: ۴ تا ۱۴).

نتیجه گیری

امنیت سایبر یک مشکل عمده برای امنیت ملی ایالات متحده است. تصمیمات و اقدامات باید حافظ حریم خصوصی و احترام به آزادی‌های مدنی باشد. ابتکار عمل بخش خصوص به تنهایی امنیت را تولید نمی‌کند. اتخاذ استراتژی جامع امنیت ملی که شامل هر دو جنبه داخلی و بین‌المللی امنیت سایبری، امنیت آمریکا را افزایش می‌دهد. مشارکت بخش خصوصی و دولتی به دلیل اختلافاتی مانند به اشتراک‌گذاری اطلاعات و مسایل غیره باعث شده تا استراتژی‌های آمریکا در این زمینه با ناکامی‌هایی روبرو شوند. ایالات متحده نیاز به مفاهیم و استراتژی جدید برای کاهش خطرات در فضای مجازی دارد. هرچند عمدتاً بر نقش دولت ایالات متحده برتقویت سایبری متمرکزشده است، اما افراد نیز نقشی مهم در این عرصه ایفا می‌کنند. مهاجمین سایبری از نقاط و منافذ متعددی برای ورود به شبکه‌های خانگی و تجاری استفاده می‌کنند، از این رو، اتخاذ اقدامات پیش‌گیرانه بسیار حیاتی است.

پیچیدگی این فضا به این معنا است که رهبران باید سیاست‌های امنیت سایبری خود را از طریق کانال‌های مختلف دنبال کنند. همان‌گونه که تنها یک سازمان دولتی در آمریکا نمی‌تواند از تمامی شهروندان حمایت کند، یک سیاست تنها نیز نمی‌تواند امنیت سایبری کاملی ارایه دهد. از این رو دولت آمریکا نیاز به این دیده است که برای تقویت امنیت سایبری خود اقدام به یک برنامه‌ریزی جامع در سطح بین‌المللی در این زمینه بنماید.

برای نیل به این مقصود، آمریکا به دنبال این است که وزارت امورخارجه با همکاری کاخ سفید، وزارت دفاع و دستگاه‌های اطلاعاتی کشور و همچنین وزارت امنیت داخلی و سایر سازمان‌های کلیدی باید قابلیت‌ها و ظرفیت‌های نهاد تازه تأسیس"دایره تأمین امنیت سایبری" جهانی را افزایش دهند. این نهاد اهداف ذیل را دنبال می‌کند:

– بررسی و شناسایی نهادهای بین‌المللی و عوامل غیردولتی که دارای تخصص لازم در عرصه امنیت فضای سایبری باشند. تجهیز و توانمند سازی سازوکارهای تأمین کننده امنیت سایبری کشور باید از طریق ایجاد همکاری با این نهادها و عوامل صورت گیرد.

– اجرای برنامه‌های کوتاه مدت شامل دنبال کردن رویکردهایی مانند تبادل اطلاعات پیشرفته، ایجاد آمادگی در برابر بحران، برگزاری مانورهای مشترک امنیت سایبری با کشورهای هم پیمان، برگزاری نشست‌های دو جانبه با موضوع امنیت سایبری و عقد توافق‌نامه‌های اعتمادسازی با کشورهای غیر هم‌پیمان.

– اجرای برنامه‌های دراز مدت شامل ایجاد توافقات چند جانبه به منظور اجرای کامل قوانین مرتبط با امنیت سایبری و تبیین هنجارها در این حوزه.

منابع

۱- دان کاولتی، میریام(۱۳۸۹). سیاست‌های تهدید و امنیت سایبری، محبوبه بیات، تهران: مرکز آموزشی و پژوهشی شهید صیاد شیرازی.

۲- دی آنجلیز، جینا(۱۳۸۳)، جرایم سایبر، ترجمه سعید حافظی و عبدال صمد خرم آبادی، تهران: شورای عالی توسعه قضایی.

۳- جلال فراهانی،امیرحسین(۱۳۸۵)،«تروریسم سایبری»،تهران،پژوهشگاه فرهنگ و اندیشه اسلامی، فصلنامه فقه و حقوق، سال سوم،شماره۱۰.

۴- چین و آمریکا، از رقابت نظامی تا سایبری(۱۳۹۰)، قابل دسترسی در: (www khabarfarsi.com.)

۵- حسن بیگی، ابراهیم. (۱۳۸۴)، حقوق و امنیت در فضای سایبر، تهران: انتشارات مؤسسه فرهنگی مطالعه‌ها و پژوهش‌های بین‌المللی ابرار معاصر.

۶- رایش، والتر. (۱۳۸۱). ریشه‌های تروریسم، ترجمه سید حسین محمدی نجم، تهران: دوره عالی جنگ، دانشکده فرماندهی و ستاد سپاه.

۷- سلیمانی فارسانی، امین(۱۳۸۸)، «انقلاب اسلامی و جنگ نرم»، نشریه پیام انقلاب، شماره۳۱ .

۸- ضیایی پرور، حمید. (۱۳۸۳)، جنگ نرم۱؛ ویژه جنگ رایانه‌ای، تهران: انتشارات موسسه فرهنگی مطالعه‌ها وپژوهش‌های بین المللی ابرار معاصر.

۹- عبداله خانی، علی،(۱۳۸۹)، جنگ نرم۳؛ نبرد در عصر اطلاعات، تهران: انتشارات مؤسسه فرهنگی مطالعه‌ها و پژوهش‌های بین‌المللی ابرار معاصر.

۱۰-کارازوجیانی، آتینا، سیاست‌های منازعه سایبری (۱۳۸۸)، مترجم محبوبه بیات، تهران: مرکز آموزشی و پژوهشی شهید صیاد شیرازی.

۱۱-کدخدایی، عباسعلی و نادر ساعد (۱۳۹۰)، "تروریسم و مقابله با آن"، تهران: مجمع جهانی صلح اسلامی.

۱۲-نای جوزف،(۱۳۹۰)، آینده قدرت، ترجمه رضامراد صحرایی، تهران: انتشارات حروفیه.

۱۳-هالپین، ادواردو دیگران،(۱۳۸۹)، جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی،ترجمه روحالله آرانی،دفترمطالعات سیاسی مرکز پژوهش‌ها مجلس.

14- Army, U. (2005) Cyber Operations and Cyber Terrorism In U. Army, U.S. Army Trainin.

15- Brett Pladna, (2007) Cyber Terrorism and Information Security http://www.infosecwriters.com

16- Chertoff, Michael (2008), The Syber security Challenge , Regulation & Governance.

17- Cornis, Paul & Livingstone, David & Clemente, Dave & Yorke, Claire (November 2010) On Cyber Warfare , A Chatham House Report, www.chathamhouse.org.uk

18- CSIS Center for Strategic & International Studies. (2011). Cyber security Two Later, A report of the CSIS Commission on

Cyber security for the 44th presidency.
19- Fritz, Jason, (2008), How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness
20- Gorman, Siebhan. (2009) Electricy GrildInvs The Wall Street Journal,8 April 2009
21- http://www.dhs.gov/files/technical/cybersecurity.shtm
22- Islam Qasem, Teun van Dongen, Marjolein de Ridder (2011), Dealingwith Cyber Security: accept vulnerability World Foresight Forum is aninitiative ofwww.worldforesightforum.org.
23- Lewis, james A. (2011), Cyber Security Two Years Later, Center forStrategic & International Studies (CSIS), available at: http://www.csis.org/publication/ cybersecurity-two-years-later, (accessed by June 13, 2011).
24- Lord, Kristin M. & Sharp, Travis (2011), America s Cyber future Security and Prosperity in the Information Age , Center for a New AmericanSecurity, Volume I.
25- Nagre, Dhanashree & Warade, Priyanka, (2008). CyberTerrorism Vulnerabilities and Policy Issues Facts Behind The Myth http://www.andrew.cmu.edu/ user/dnagre/
26- Nye, Joseph s. (2010), Cyber Power , Belfer Center for Science and International Affairs.
27- Nye, Joseph S, Jr., (2011), Power and National Security in Cyberspace ,Center for a New American Security.
28- Nye, joseph, (2010), The Future of American power ,oreign Affairs.
29- Rodriguez, Carlos A. (2006) Cyber terrorism Inter-American Defense College as a prerequisite for the Diploma approved.
30- Stone, Marianne. (2010) Obama, sCyber security Plan ColumbiaUniversity, school of international and public affairs New York.
31- Theohary, Catherine A. & Rollins, Johan (2009), Cyber Security: Current Legislation, Executive Branch Initiative, and Options for Congress Congressional Research Service.
32- Vatis, Michael (2002), Cyber Attacks: Protecting American s SecurityAgainst Digital Threats , John F. Kennedy School of Government, Harvard University.
33- White House. (2011). Internationa Straregy for Cyberspace, Prosperity, Security, and Openness in a Networked World.