ویژگی‌های حملات سایبری و راه‌های کنترل آنها از طریق ایجاد کنوانسیون قوانین سلاح‌های سایبری

بهمن ابراهیمیان[1]، علی توشه[2]

[1] مدرس مدعو، گروه مهندسی فناوری اطلاعات، دانشگاه پیام نور

رشت، ایران

Bahman.ebrahimian@modares.ac.ir

[2] دانشجوی کارشناسی ارشد، دانشگاه امام حسین(ع)

تهران، ایران

Ali.tosheh@yahoo.com

چکیده

امروزه اینترنت امکانات بسیار زیادی را در رفع نیازهای انسان‌ها فراهم کرده است، اما اینترنت فضای گسترده‌ای سرشار از نامنی است و در گستره‌ء جهانی آن که از شبکه‌های مختلف و ناهمگون تشکیل شده است انواع مختلف حملات سایبری وقوع می‌یابد. در این مقاله ضمن بررسی انواع حملات سایبری و ذکر نمونه‌هایی از آنها، به تجربه نسبتا موفق معاهده‌های بین‌المللی در جلوگیری از تولید و استفاده سلاح‌های شیمیایی، هسته‌ای پرداخته و شرایط لازم برای ایجاد چنین معاهده‌ای برای کنترل ابزارهای مورد استفاده در حملات اینترنتی و راه‌های مقابله مورد بررسی قرار می‌گیرد. در نهایت راه‌کارهای کاهش خطرات ناشی از حملات سایبری از طریق ایجاد معاهده‌ای بین‌المللی بیان می‌شود.

کلمات کلیدی:

فضای سایبر، حمله سایبری، امنیت، قرارداد.

۱- مقدمه

از دیرباز تهدیدهای گوناگونی کشورهای جهان را به واسطه توسعه تسلیحات جنگ افزاری تهدید می‌کند. پس از وقوع چندین جنگ خانمانسوز، بسیاری از کشورهای جهان نیاز به وجود قراردادهایی به منظور منع گسترش، تولید و به کارگیری سلاح‌های غیرمتعارف مانند سلاح‌های شیمیایی ، اتمی و ... را احساس کردند و با توجه به توافقات صورت گرفته، معاهده‌هایی را به منظور رعایت همه کشورهای عضور تنظیم کردند. از سوی دیگر در دنیای امروز نوع تقابل و سلاح‌های مورد استفاده برای حمله یک کشور به کشورهای دیگر متنوع‌تر شده است و هرچه زمان می‌گذرد چالش ایمن کردن اینترنت بدتر می‌شود[1] . رشد روز افزون اینترنت و وابسته شدن بیش از پیش دولتها به آن موجب شده است تا مسئله امنیت در برابر حملات سایبر[1] یکی از دغدغه‌های اساسی دولتها باشد. تا کنون حدود ۱۰۰ گونه آسیب در فضای سایبر شناسایی شده است[2].

به طور کلی حملات سایبری عبارتند از فعالیتهای یک عامل خودی یا بیگانه که انتظارات امنیتی را برای یک فرد و یا سازمان قابل سازش و منعطف می‌کند. بعضی از حمله ها ناشی از مناقشات سیاسی هستند در حالیکه بعضی دیگر از دیدگاههای متفاوت اجتماعی سر چشمه می‌گیرند. برخی از آنها بخاطر باورهای سیاسی،افراط گرایی و انتقام و خشم صورت می‌پذیرند. بنابراین نقش عامل های انسانی در این حملات به شدت پر رنگ می‌باشد[3].

باوجود تمام تلاشی که مدیران شبکه برای توسعه سامانه‌های حفاظتی انجام می‌دهند؛ باز هم خطرات بسیاری شبکه های کامپیوتری را تهدید می‌کند چرا که نفوذ، بهره‌برداری و یا تخریب این شبکه‌ها منفعت بسیاری برای حمله‌کنندگان[2] و نفوذگران[3] دارد. درواقع درصورتی که جنگی بین دو یا چند کشور یا ابرقدرت رخ دهد یکی از جنبه‌های آن جنگ در عرصه اینترنت خواهد بود. چرا که در یک طبقه بندی کلی، ابزارهای حمله سایبری[4] به نسبت سایر ابزارهای جنگی عمومی، بسیار بیشتر در اختیار کشورها قرار دارند و هزینه استفاده آنها کمتر و روشهای استفاده از آنها سهل‌تر می‌باشد. ضمن آنکه بسیاری از تروریستها می‌توانند با استفاده از امکانات قابل توجه این ابزارها مخاطرات بسیار زیادی را برای دولتهای گوناگون ایجاد کنند[4].

مسلماً بهترین راهکار برای در امان ماندن از حملات اینترنتی، قطع مسیر دسترسی به اینترنت می‌باشد. اما با توجه به فواید بسیار زیاد اینترنت و وابستگی روزافزون به به آن، چنین امری غیرممکن است. به نظر می‌رسد بروز چنین مشکلاتی باعث شود تا پیمانهایی در خصوص جلوگیری از گسترش حملات اینترنتی در سطح بین‌المللی ایجاد گردد.

ایجاد کنوانسیون[5] سلاح های سایبر[6] یکی از استراتژی های ممکن است؛ مانند قراداد سلاح های شیمیایی که در سال ۱۹۹۷ مدلی قوی را در راستای منع توسعه، تولید، ذخیره و استفاده از سلاح های شیمیایی و قراداد تخریب آنها ایجاد نمود[5].

اگر نگاهی بر قرارداد منع گسترش سلاح‌های شیمیایی داشته باشیم می‌بینیم هدف آن استفاده منحصر به فرد از دستاوردهای شیمیایی برای اهداف سودمند و منع استفاده تسلیحات شیمیایی به منظور نجات تمام بشر است. هر امضاکننده این قرارداد مسئول اجرا ی « قرار داد منع توسعه، تولید، ذخیره و استفاده از سلاح های شیمیایی و قراداد تخریب آنها» در قلمرو قانونی خود است و باید تمامی تسلیحات شیمیایی و امکانان تولید آنرا تخریب کند. مقر سازمان منع سلاح های شیمیایی[7] در شهر لاهه قرار دارد. این سازمان نهادی مستقل است که هماهنگ با سازمان ملل فعالیت می‌کند. Opcw ، ۵۰۰ کارمند و بودجه ای به میزان ۷۵ میلیون یورو دارد. به طور رایج ۱۸۸ ملت که دارای ۹۸٪ از جمعیت جهان هستند، عضوی از این سازمان هستند.

۲- انواع حمله‌های سایبری

به طور کلی حمله‌های سایبری با مقاصد گوناگون و به صورتهای مختلف صورت می‌گیرند. در ادامه به بررسی انواع حمله‌های سایبری می‌پردازیم[6].

۲-۱- حمله هایی که با اهداف سیاسی صورت می-پذیرند

مجرمان سایبری که در حملات با انگیزه های سیاسی شرکت داشته اند، ممکن است عضوی از گروههای افراطی که جهت نشر و گسترش

[1] Cyber attack
[2] attackers
[3] hackers
[4] Cyber attack tools

[5] Convention
[6] Cyber Weapons
[7] Opcw: Organization for the Prohibition of ChemicalWeapons

تبلیغات، حمله به وب سایتها و شبکه های دشمن، سرقت پول جهت تامین مالی فعالیتهای خود و یا کشیدن نقشه و هماهنگی جهت انجام آنها در دنیای فیزیکی استفاده کنند . این حملات در گروه های زیر ودسته بندی می‌شوند که برای هر یک نمونه‌ای نیز ذکر می‌گردد.

۲-۱-۱- اعتراضات سیاسی به اقدامات دولت

نمونه : جون ۱۹۹۸ هند، حمله به یک مرکز اتمی : هکر هایی از امریکا، انگلیس، هلند،و نیوزلند به وب سایت مرکز تحقیقات اتمی (BARC) جهت اعتراض به آزمایشهای اتمی حمله بردند. حمله کنندگان با ارسال متنهایی به وب سایت آنرا تخریب اطلاعاتی کردند.

۲-۱-۲- نارضایتی از آغاز یک سیاست ، قانون و یا سند عمومی

نمونه : دسامبر ۱۹۹۵، فرانسه، حمله سایبری علیه وب سایت دولت فرانسه: گروهی به نام Strano network یک اعتصاب شبکه‌ای را به مدت یک ساعت با تشویق معترضان به باز کردن سایت دولت فرانسه با مرورگرهایشان، و به منظور اعتراض به سیاستهای اتمی و اجتماعی این دولت آغاز کردند. با این کار حجم بزرگی از ترافیک وبی ایجاد شد و این وب سایت غیرقابل دسترس گردید.

۲-۱-۳- تعدی بر ضد فعالیتهای مربوط به خشونتهای فیزیکی

نمونه : می۱۹۹۵ بلگراد، بمبگذاری سفارت چین: هکرهای چینی سایتهای دولت امریکا را به علت بمبگذاری تصادفی در سفارت چین واقع در بلگراد مورد حمله قرار دادند.

موارد دیگر را بدون ذکر نمونه صرفاً نام می‌بریم:

- حملات با منشا اجتماعی فرهنگی
- حملات با منشا اختلافات مرزی و سرزمینی
- حملات با منشا سالروزهای خاص یا وقایع تاریخی
- حملات با انگیزه های اقتصادی
- حملات جاسوسی (سیاسی /اقتصادی)

۳- به تصویر کشیدن حملات سایبری

نگاه اول بطور کلی نشان می‌دهد که انگیزه‌های سیاسی و اجتماعی، فراوانی بیشتری نسبت به انگیزه های مالی و اقتصادی در تعداد حمله‌ها دارند.

نگاه دیگر، بررسی عوامل جغرافیایی حمله‌ها است. فقدان این حملات در کشورهای امریکای جنوبی و استرالیا به علت بستر سیاسی پایدار و در افریقا به دلیل مناقشات سیاسی و فرهنگی و کمبود زیرساخت های فناوری، قابل توجیه می‌باشد.

نگاه آخر بررسی عامل زمان در حمله هاست و نشانگر این است که با گذشت زمان شکل ظاهری حمله‌ها تغییر می‌کند . در گذشته به علت فقدان امنیت کافی در زیرساختهای نرم افزارهای وب ، گرایش به حمله مستقیم به وب سایتها بیشتر دیده می‌شد . اما امروزه حملات سایبری متفاوتند و بیشتر از نوع حمله های(DDoS2) هستند که توسط افراد خبره و به‌کارگیری تعداد زیادی کامپیوتر جهت حمله به دشمنان سیاسی انجام می‌پذیرند.

۴- ابعاد حمله

در اینجا به بررسی ابعاد گوناگون یک حمله سایبری می‌پردازیم.

۴-۱- عوامل حمله

در حمله‌های سایبری این سیستمهای کامپیوتری هستند که بصورت مستقیم در حمله شرکت دارند، اما در پشت هر حمله یک عامل انسانی با یک انگیزه وجود دارد. شناخت انواع مهاجمان اصلی‌ترین و اساسی-ترین جز در ابعاد سایبری است. از آنجایی که عوامل انسانی اولین نقطه تلاقی بین وقایع دردنیای فیزیکی و وقایع در دنیای سایبری هستند، آگاهی از وجود حمله و نظارت دقیق (مانیتورینگ) اختلافات و تغییرات در تعداد معینی از حمله کنندگان از نوع مشخصی از حمله، که سر منشا خاصی دارند، می‌تواند به عنوان راه حلی کلیدی جهت پیش بینی حمله های سایبری بکار برده شود.

عامل انسانی که در یک حمله سایبری مقصر است می‌تواند بطور گسترده به چهار گروه طبقه بندی شود:

• کاربران آماتور (جهت تفریح ، مهارت پایین)

• مزدوران و سودجویان(هک بخاطر پول، سازماندهی شده، ماهر)

• معترضان اجتماعی (هکتیویستها، بطور آزادانه سازماندهی شده)

• گروههای قومی - ملیتی (هک بخاطر یک هدف, بسیار ماهر و تامین از لحاظ مالی)

۴-۲- هماهنگی حمله

حمله های سایبری عظیم معمولا با گروههایی از عوامل انسانی که بصورت متحد فعالیت می‌کنند؛ ارتباط دارند . هماهنگی و همکاری حمله های سایبری را می‌توان به دو دسته تقسیم بندی کرد:

• حملات سازماندهی نشده- ناهماهنگ

• حملات سازماندهی شده- هماهنگ

گروههای سازماندهی نشده ازمسایلی همچون نژاد پرستی، میهن پرستی و مسائل حساس و عاطفی جهت نفوذ و انگیزش مشارکتها اسفاده می‌کنند. این گروهها همچنین بطور نامحسوس با شبکه های اجتماعی همانند چت رومها و فرومها و وبلاگها در ارتباط هستند.

در مقابل، حملات سازماندهی شده شامل فعالیتهای بسیار هماهنگ در بین گروهی از افرادبا تعامل بسیار نزدیک است، که بصورت پنهانی با یکدیگر همکاری می‌کنند.این گروهها شامل سندیکاهای مجرمین و یا گروهی از افراد که توسط دولت یا ارتش، مشخصا جهت اغاز یک حمله استخدام گردیده اند می‌باشند .

۴-۳- خاستگاه و مبدا حمله‌ها

مبدا و خاستگاه حمله، چالشی بسیار مهم برای امنیت سایبری است . تمرکز زدایی هایی که با فرمانهای (peer-to-peer) و کنترل شبکه ها انجام می‌پذیرند ، می‌توانند مبدا حمله های سایبری را مبهم کنند. با این حال هنوز هم ردیابی شبکه های انسانی که در نهایت مسئول آغاز یک حمله هستند تقریبا غیرممکن است، مگر اینکه شخص یا گروهی مسئولیت حمله را بر عهده بگیرد.

۴-۴- قربانیان حمله

معمولاً افراد هدف حمله های سایبری بزرگ نیستند، بلکه زیرساختها ،هدف اصلی این حمله ها هستند که عواقب چنین حمله ای می‌تواند بسیار گسترده باشد. بر خلاف حمله های سایبری بزرگ، حمله ها در اندازه های کوچک، کاربرانی را هدف قرار می‌دهند که از آسیب پذیری سیستمهای فنی نا آگاهند .این کاربران ممکن است بی تجربه، ناتوان و یا از نظر احساسی ضعیف باشند.

۴-۵- عواقب حمله

گوناگونی عواقب حمله با ابعاد SPEC مشابه است و می‌تواند تاثیرات روانی بر جامعه گذاشته و باعث ترس و وحشت گردد و همچنین می‌تواند باعث تحمیل مخارج هنگفتی به کشور شود، مانند غیر ممکن شدن دسترسی به زیرساختهای بخشهای قابل توجهی از فضای سایبری توسط حملات DDOS.

۴-۶- پاتولوژی منشا حمله‌های سایبری

دفاع سایبری از قانون شکنی سایبری مشکل تر است. ما نیازمندیم که همه جوانب و عواملی که موجب شکل گیری و تغییر امنیت محیط سایبری می‌شود را مورد بررسی قرار دهیم، از آن جمله می‌توان عوامل سیاسی، اقتصادی ، فرهنگی و گرایشهای تکنولوژیکی را نام برد. رواج فرهنگ امنیت سایبری باعث کمک به رشد اقتصاد کشورها می‌شود واین فرهنگی است که در راستای سازگارنمودن فن آوریها ، فرآیندها و انسان ها، با امنیت سایبری گام بر می‌دارد.

۵- گام‌های ایجاد نظام کنترل سلاح‌های سایبری

دولت ها برای جلوگیری از تهدید تسلیحات شیمیایی ، سازمان منع تولید تسلیحات شیمیایی را ایجاد و گسترش دادند.

باید توجه نمود که سلاح های سایبر ، مانند سلاح های شیمیایی نیستند. اگرچه شباهت هایی با آن دارند؛ مانند اینکه دستیابی به آنها آسان است، خسارت بی تناسبی[1] دارند، و چند ریختی[2] هستند؛ اما تاکتیک ها ، استراتژی ها و تاثیرات آنها به طور بنیادی با سلاح های شیمیایی متفاوت است. هدف استفاده از سلاح‌های شیمیایی نیروی انسانی است اما سلاح های سایبر[3] ماشین‌ها و اطلاعات را مورد هدف قرار می‌دهند. از نظر شیوه تهدید نیز در هنگام جنگ یک حملهء شیمیایی امنیت کشور را به طور کاملا آشکار به مخاطره می‌اندازد اما حمله ی سایبر امنیت ملی را به طور پنهانی تهدید می‌کنند.

بنابراین احتمال تشکیل سازمانی که بر نحوه استفاده از ابزارهای حمله سایبری نظارت کند، بسیار قوی به نظر می‌رسد.

حال نکاتی را که باید در ایجاد یک رژیم حقوقی وضع قوانین سایبر رعایت شود را به اختصار در جدول ۱ بیان کرده و به تشریح موارد آن به صورت زیر می‌پردازیم.

[1] Asymmetric damage
[2] polymorphism
[3] Cyber weapones

۵-۱- فراگیری و اجماع

هر چند جامیعت قانون انگیزه استفاده از آن را افزایش می‌دهد اما در نگاه اول این استراتژی می‌تواند مانعی برای پیشرفت وضع قوانین به نظر آید. اما زمانیکه اعضای این قرارداد احساس امنیت بیشتری نسبت به غیر عضوها داشته باشند؛ تمایز بین دولتها و افراد عضو با غیر عضوها روشن شده و تمایل به عضویت در این قرارداد بیشتر می‌شود.

قراردادهای بین المللی به توافق گسترده ای در مورد ماهیت مشکل عام نیاز دارد. ترسی که تروریست ها از تسلط بر روش‌های نفوذگری[1] نفوذگری[1] ایجاد می‌کنند؛ می‌تواند آنقدر قوی باشد که چنین توافق سیاسی را ایجاد کند؛ مانند زمانی که یکی از شهرهای امریکا در خاموشی واقع شد و اقای اوباما وقوع آن را به حملات سایبری نسبت داد. هرچند بسیاری از رسانه‌ها وقوع آن را به برزیل نسبت دادند اما هنوز منبع حملات مشخص نشده است[7].

ایجاد چنین قراردادی که قصد دارد به ایمن کردن اینترنت کمک کند، به مشارکت قدرتهای بزرگ دنیای امروز مانند آمریکا، روسیه، چین و انگلیس نیاز دارد.

جدول ۱- گام‌های ایجاد نظام کنترل سلاح‌های سایبری [4]	
فراگیری و اجماع	• لزوم ایجاد حس نیاز به امنیت سایبری در کشورها از طریق روشه‌های مختلف اطلاع رسانی • ایجاد احساس امنیت بیشتر در اعضای قرارداد نسبت به غیر عضور در برابر حملات سایبری
کمک و یاری رسانی	• کمک به کشورها از طریق برگزاری آموزش‌های تخصصی • ایجاد برنامه‌هایی به منظور تمرین‌های مدیریت خطر، آموزش آگاهی، دفاع عمقی • یاری رسانی به کشور قربانی[2] در مقابل حملهسایبری کشور متخاصم و تنبیه متخاصم

جدول ۱- گام‌های ایجاد نظام کنترل سلاح‌های سایبری [4]	
منع	• بستن راههای نفوذ به شبکه های کامپیوتری با به کار بستن ابزارهای مناسب • در اختیار داشتن اهرم های مناسب به منظور ممانعت کشورها یا مجرمین از دسترسی به ابزارهای حملات سایبری

۵-۲- کمک و یاری‌رسانی

سازمان های دولتی هیچ راهی جز سرمایه گذاری زمان و تلاش بیشتر در ایمن‌سازی کامپیوتر ندارند. چنین سازمانهایی باید بتواند به ایجاد دوره‌های اموزشی تخصصی توسط خبرگان این امر به سطح دانش کارشناسان امنیت کشورها کمک کند. این کار با آموزش متخصصان محلی ممکن است.

بهترین تمرین ها مثل : مدیریت خطر، آموزش آگاهی، دفاع عمقی، و حل کردن یک حادثه معمولا به کارشناسی و منابعی بیشتر از آنچه که بیشتر سازمان ها و حتی بسیاری از کشورها دارند، نیاز دارد.

جنبه دیگر یاری‌رسانی زمانی است که کشوری توسط کشور دیگر موجب تهاجم سایبری قرار گیرد که در اینصورت سازمان باید به کمک کشور قربانی در برابر کشور متخاصم بپردازد.

متخصیصن می‌توانند توصیه های تکنیکی، قانونی و سیاسی را از طریق مشاوره و آموزشی تهیه کنند. گروه واکنش بحرانی می‌تواند برای گسترش جهانی در زمان تشخیص در دسترس باشد و برای انتشار یافته‌هایش در سراسر جهان آماده باشد. این موسسه می‌تواند به طور فعال فواید استفادهء سودمند از تکنولوژی کامپیوتر برای پیشرفتها و همکاری‌های اقتصادی را ارتقا بخشد. اقدامی مهم اما دشوار، برای دولت ها که باید آن را انجام دهند تنظیم ابزار متصل و بررسی اینترنت و ترافیک شبکه اش است.

خیلی از تهدیدهای فضای سایبر مثل تهدیدی که با تکنولوژی botvet ایجاد شد، خیلی سریعتر از تهدیدهای ایجاد شونده توسط سلاح‌های معمول است. کاهش حملهء سایبر به شناسایی فوری منبع و عبور سریع از مرزهای تکنیکی، قانونی و ملی نیاز دارد. بهترین شانسی که تصویب کنندگان قرارداد سلاح های سایبر[3] در آینده خواهند داشت، دسترسی آنها به داده های شبکه در زمان واقعی از سرتاسر اینترنت است و همچنین توانایی همکاری فوری با

[1] hacking
[2] victim
[3] cyber weapons convention

کارشناسان خود در سراسر جهان است. نکته مهم بحث اقتدار ملی و اهمیت خصوصی بودن داده‌ها است که باید با دقت محافظت شوند.

۵-۳- منع

چنین سازمانی باید بتواند با مطالعه رویکردهای اتخاذ شده توسط سازمان‌هایی نظیر منع گسترش سلاح‌های هسته‌ای و .. به اهرم‌هایی دست پیدا کند تا بتواند کشورهای عدول کننده از قوانین را وادار به رعایت و تمکین نماید. دستیابی به چنین امری با وضع قوانین محکم و مورد اجماع توسط اکثر کشورها ممکن خواهد بود.

به عنوان مثال در ماه می‌سال ۲۰۰۹ ، لابراتور ضد ویروس kaspersky حدود ۵۲۰ /۴۲ انواع برنامهء «ناخواستهء پتانسیلی و تبلیغاتی مضر و منحصر به فرد»[1] در کامپیوتر مشتری هایش یافت[8] . حتی در شبکه ای با اطلاعات آزاد که به خوبی طراحی شده است می‌توان با استفاده از هکری ناشناس ، مسیری قانونی برای ادارهء سیستم از دور ایجاد کرد. یک راه، دزیدن رمز عبور یا حدس زدن آن است. هر برنامه نویس حرفه‌ای کامپیوتر می‌تواند برنامه نویسی مرتبط با هک کردن را یاد بگیرد و افرادی که برنامه نویس نیستند می‌توانند به سادگی ابزارهای حمله سایبری را با کیفیت حرفه ای از وب سایت‌های معرف دانلود کنند. به‌علاوه جنگاوری سایبری با جنگاوری سلاح‌های شیمیایی متفاوت است به این صورت که یک مهاجم فضای سایبر اغلب به طور پنهانی و به صورت گمنام و ناشناس حمله می‌کند.

بنابراین این کار زمان‌گیر است و نیازمند همکاری‌های تکنیکی ، قانونی و بین‌المللی در سطحی خیلی بالاتر از سطح امروز است.

۵-۴- بازرسی

باید بتوان مانند سایر رژیم‌های حقوقی حق تقاضای «بازرسی چالشی» را براساس قانون «هر زمان، هر جا» است را برای سازمان در نظر گرفت و هیچ کشور عضوی حق رد کردن آن را نداشته باشد.

البته پیاده سازی این امر در فضای سایبر بسیار دشوار است. به عنوان مثال حافظه فلش ۲۵۶ گیگا بایتی، چیزی کمتر از ۱۰۰۰ دلار قیمت داشته و می‌تواند شامل بیش از ۲ تریلیون اطلاعات باشد. در آن صورت تجزیه و تحلیل چنین حجم عظیمی از اطلاعات حتی با مشارکت متخصصین این امر به آسانی امکان پذیر نیست[9].

به طور کلی، قرارداد سلاح‌های سایبری باید بتواند بازرسی دقیق‌تر سرویس دهندگان خدمات اینترنتی[2] را مد نظر قرار دهد. هم اکنون قراردادهایی در این زمینه موجود هستند مانند قرارداد اروپا در مورد جرم سایبر و SORM روسیه. هرچند که هر کدام از اینها از نظر الگوریتم و اجرا منحصر به فرد هستند اما همهء آنها با مشکلی به نام ترافیک شبکه مواجه هستند.

۶- نتیجه گیری

با توجه به مخاطراتی که در حال حاضر در عرصه فضای سایبر وجود دارد لزوم امن سازی آن بیش از پیش ملموس است. حملات گوناگونی توسط ابزارهای سایبری قابل انجام است که جلوگیری از آنها نیازمند وضع قوانین دقیق، شفاف و کاربردی است. زمانی وضع این قوانین می‌تواند مفید باشد که اجماع کاملی توسط اکثر کشورهای بین‌المللی و به طور خاص کشورهای مطرح در این زمینه ایجاد شود و ضمانت اجرایی لازم برای ایجاد قوانین آن مانند سرکشی‌های ناگهانی و پایش وضعیت امنیتی آنها وجود داشته باشد. انجام این امر با توجه به مباحث امنیت ملی و محرمانگی اطلاعات خصوصی افراد، قدری دشوار است.

برای ایجاد رژیمی که بتواند نیازهای گفته شده در این مقاله را برآورده کند لازم است به چگونگی تدوین و اجرای معاهده‌هایی از این دست، پرداخته شود.

مراجع

[1] Geers K. *A Brief Introduction to cyber warfare. Common Defense Quarterly*; 2010, Spring.
[2] Online document, available: http://cve.mitre.org
[3] Fulghum DA, WallR,ButlerA. *Cyber combat' sfirsts hot.*Aviation Week & Space Technology 2007;167(21):28
[4] Geers K. *Cyber Weapons Conventions* ; 2010, Computer Low and Security review.
[5] Newmark J. *Chemical warfare agents: a primer*. Military Medicine 2001.
[6] Geers. K. *The challenge of cyber attack deterrence.* computer law & security review 26 (2010).
[7] Gray DH, Head A. *The importance of the internet to the post-modern errorist and its role as a form of safe haven. European.* Journal of Scientific Research 2009;25(3): 396e404.
[8] Monthly Malware Statistics. Kaspersky Lab website, www. kaspersky.com; Jun 2011.
[9] Cole E. Hackers Beware. London: New Riders; 2002.

[1] spam

[2] ISP: Internet Service Provider