برخی حوزه‌ی مجازی را پنجمین حوزه از نبرد می‌دانند .تحلیل‌گران نظامی، حوزه‌ی مجازی را به عنوان یک دامنه‌ی جدید در حوزه‌ی جنگ به رسمیت شناخته‌اند که اهمیت آن در حال حاضر در حال فزونی گرفتن از سایر حوزه‌هاست. وجود نداشتن قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا برضد کشور دیگر وارد جنگ مجازی شود ...

»با آنکه از نظر واردات ارتباطاتی، ایران سخت‌ترین محدودیت‌ها را دارد با این حال، تکنولوژی‌های اطلاعاتی در این کشور در سطح بالایی قرار دارند و ایران در کنار روسیه از قدرتمندترین کشورها در زمینه‌ی جنگ مجازی محسوب می‌گردد(CNNreport, February 2003) «.

فضای مجازی فضایی است که قوانین خاص خود را دارد. امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها در حال حاضر، از جمله امکانات دولتی و خصوصی، بانک‌داری و امور مالی، حمل‌ونقل، تولید، پزشکی، آموزش و پرورش و دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. فضای مجازی ابزاری برای قدرت و ثروت است. اگر از آن استفاده نکنیم دیگران از آن استفاده خواهند کرد و آن هم برضد ما. گاهی به دلیل ناشناخته بودن منبع حمله؛ فضای مجازی به مکانی ایده‌آل برای جنگ تبدیل شده است .برآورد سال گذشته نشان می‌دهد که دولت آمریکا از محل حملات سایبری در جهان، 100میلیون دلار خسارت دیده است.

جنگ مجازی اشاره به درگیری‌ها در فضای مجازی با اهداف سیاسی و ایدئولوژیک دارد. این مفهوم به جنگ اطلاعاتی اشاره دارد، درست به مانند جنگی واقعی که البته در مورد انگیزه‌های این جنگ و جنگ واقعی اختلاف نظر وجود دارد. تعریف دقیق جنگ مجازی به «اقدام‌های انجام شده توسط دولت یک کشور و سایر افراد به منظور نفوذ در رایانه‌ها و شبکه‌های سایر کشورها جهت اقدام‌های تخریب و آسیب اشاره دارد که این روش از راه روش‌های الکترونیکی صورت می‌گیرد.» کشورهایی با فناوری و متخصصان عقب مانده از قافله‌ی جهانی، بازنده‌ی جنگ مجازی هستند. این جنگ می‌تواند اقتصاد را فلج کند، موجب درگیری‌هایی در داخل و خارج کشورها گردد و بهره‌وری نیروی نظامی را کاهش دهد.

هدف از حمله‌ی سایبری، دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیر ساخت‌ها مانند: «آب، برق، حمل‌ونقل و...» به نحوی که هزینه‌های اقتصادی را افزایش دهند. در ۵ سال گذشته میزان حملات سایبری در سطح جهان بسیار افزایش یافته است.

نقطه‌ی شروع برای جنگ مجازی را جنگ «بالکان» می‌دانند که نیروهای متخاصم سعی در نفوذ به اطلاعات یک‌دیگر داشته‌اند. امروزه رشد شبکه‌های رایانه‌ای بسیار سریع‌تر از رشد نرم‌افزارهای امنیتی مرتبط به آن‌هاست.

هنوز زیر ساخت‌های کافی برای جلوگیری از حملات سایبری در سیستم‌های رایانه‌ای کشورها تعبیه نشده است. فضای مجازی به یک مکان بالقوه برای جرایمی این چنینی تبدیل شده است. میلیاردها دلار بدون کمترین امنیتی در فضای سایبر روزانه جابه‌جا می‌شوند و بخشی از مهم‌ترین اطلاعات دولتی و شخصی بدون کمترین امنیتی در فضای مجازی وجود دارند که خطر حملات سایبر را افزایش می‌دهند.

برخی حوزه‌ی مجازی را پنجمین حوزه از نبرد می‌دانند .تحلیل‌گران نظامی، حوزه‌ی مجازی را به عنوان یک دامنه‌ی جدید در حوزه‌ی جنگ به رسمیت شناخته‌اند که اهمیت آن در حال حاضر در حال فزونی گرفتن از سایر حوزه‌هاست. درست به مانند ابعاد دیگر درگیری نظامی مانند، زمین، دریا، هوا و فضا.

وجود نداشتن قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا برضد کشور دیگر وارد جنگ مجازی شود. در حال

حاضر کشور ایالات متحده در جهان مرکز فرماندهی فضای مجازی را در پنتاگون راه اندازی کرده است که هدف از ایجاد آن حمله به شبکه‌های سایر کشورها و دفاع در مقابل حملات مجازی است. همچنین آژانس امنیت اطلاعات و شبکه‌ی اروپا[۱] نیز چنین مرکزی است.

در سال ۲۰۱۱م. مجله‌ی «اکونومیست» نوشت که چین برنامه‌ی ویژه‌ای دارد تا در نبرد اطلاعاتی قرن بیست و یکم، پیروز گردد. همچنین این مجله بیان داشت که سایر کشورها مانند اسراییل، روسیه و کره شمالی برنامه‌ی ویژه‌ای برای جنگ مجازی دارند که در این بین باید گفت که ایران دومین قدرت بزرگ در عرصه‌ی نبرد مجازی است. گویا این جنگ خیلی وقت است که برضد کشور ما شروع شده است. هنوز اخبار مبتنی بر حمله‌ی ویروس «استاکس نت» به تأسیسات اتمی نطنز از سر زبان‌ها نیفتاده بود که خبر مربوط به حمله‌ی ویروس »فلیم»[۲] بر صدر اخبار جای گرفت.

در ابتدا بیان شد که این ویروس یک ویروس جاسوسی است اما اکنون با اطلاعات به دست آمده بیان می‌شود که این ویروس در واقع هدف خراب‌کاری داشته است. خراب‌کاری یکی از اهداف جنگ سایبری است. در سال ۲۰۱۲م. «نیویورک تایمز» گزارش داد که اوباما رئیس‌جمهور ایالات متحده دستور حمله‌ی سایبری به تأسیسات اتمی ایران را صادر کرده است.

انواع تهدیدهای مختلف ناشی از جنگ سایبر

1. جاسوسی و نقض امنیت ملی؛

جاسوسی سایبر به عملی اشاره دارد که به منظور به دست آوردن اسرار (حساس، اختصاصی و یا اطلاعات طبقه‌بندی شده) از افراد، رقبا، گروه‌ها، دولت‌ها و دشمنان، برای استفاده‌ی نظامی، سیاسی یا اقتصادی با استفاده از روش‌های بهره‌برداری غیر قانونی در اینترنت، شبکه، نرم‌افزار و یا رایانه صورت می گیرد.

2. خراب‌کاری[۳]؛

فعالیت‌های نظامی که با استفاده از ماهواره و رایانه برای اختلال در تجهیزات دشمن صورت می‌پذیرد، خراب‌کاری نام دارد. زیرساخت‌های برق، آب، سوخت، ارتباطات، حمل‌ونقل و ... ممکن است در جنگ مجازی در معرض خطر باشند. سایر تهدیدها می‌تواند شامل سرقت اطلاعات کارت‌های اعتباری، اختلال در برنامه‌ی قطارها و یا حتی بازار سهام باشد.

3. شبکه‌ی برق.

شبکه‌های انتقال برق به دلیل وابستگی به فضای مجازی و اینترنت از مهم‌ترین هدف‌ها در جنگ مجازی محسوب می‌شوند. در سال ۲۰۰۹م. دولت ایالات متحده بیان داشت که دولت‌های چین و روسیه قصد داشتند تا با نفوذ نرم‌افزاری در شبکه‌های برق در این کشور در آن اختلال ایجاد کنند. از سوی دیگر و در نقطه‌ی مقابل نیز حملات نظامی به شبکه‌های انتقال برق برای از کار انداختن اینترنت از موارد مورد توجه در جنگ مجازی است.

انگیزه‌های جنگ سایبر

1. مقاصد نظامی؛

درست مانند جنگ واقعی در اینجا بر خلاف ۴ رکن دیگر جنگ که پیش‌تر بیان داشتیم، این جنگ در سایه‌ی فضای مجازی صورت می‌پذیرد. در اینجا به یک مرکز فرماندهی جنگ سایبر نیاز است و نیازمند سلاح‌هایی مجازی و دفاعی هستیم تا جلوی حمله گرفته شود و ما نیز قادر به حمله‌ی متقابل باشیم.

2. اهداف غیر نظامی؛

این امر عبارت از اختلال در سرویس دهنده‌ی وب، سیستم‌های اطلاعات سازمانی، سیستم‌های سرور، لینک‌های ارتباطی،

تجهیزات شبکه و رایانه‌های رومیزی و لپ‌تاپ‌های خانگی و امور تجاری است که گاهاً برای کسب انگیزه‌های تجاری رقابتی و یا مالی صورت می‌پذیرد و گاهی نیز خراب‌کاری به دلیل صرفاً سرگرمی است.

3. اهداف شخصی.

باید باور کرد که بیش از 90درصد حملات سایبر برای اهداف شخصی صورت می‌گیرد. بسیاری از حملات برای جلب توجه رسانه‌ها انجام می‌شود. شرکت (McAfee) می‌گوید، روزانه با میلیون‌ها جنبه از این نوع حملات سایبر توسط نرم‌افزارهای امنیتی‌اش روبه‌رو می‌شود.

نمونه‌هایی از جنگ مجازی

- در سال ۲۰۰۶م. در جریان جنگ حزب‌الله و اسراییل، دولت صهیونیستی اعلام کرد که مورد حملات سایبری سازمان یافته از طرف کشورهای خاورمیانه و روسیه قرار گرفته است.

- در سال ۲۰۰۷م. این بار کشور «استونی» بود که خبر از حمله‌ی سایبری به خود داد. هدف این حمله گویا رسانه‌ها، بانک‌ها و وزارتخانه‌های کشور استونی بودند که از سوی سروری در روسیه مورد حمله قرار گرفتند.

- در سال ۲۰۰۷م.، تارنمای انتخابات کشور «قزاقستان» در جریان یک حمله‌ی سایبری از کار افتاد.

- در سال ۲۰۰۸م.، سایت‌های کشورهای روسیه، گرجستان و آذربایجان در جریان درگیری‌ها در اوستیای جنوبی مورد حمله‌ی هکرها قرار گرفتند.

- در سال ۲۰۰۹م.، حملات گسترده‌ای به بخش‌های دولتی، رسانه‌ای و تارنماهای مالی دو کشور ایالات متحده و کره جنوبی صورت پذیرفت. در حالی که همه به راه‌اندازی حمله از سوی کره شمالی نظر داشتند یک تحقیق نشان داد که با کمال تعجب حمله از یک سرور ناشناخته در بریتانیا بوده است.

- در ماه می 2010م.، در پاسخ به حمله‌ی سایبری هند، تارنماهای سازمان موشکی هند، بنیاد ملی علوم هند، دفتر چندین حزب و ... مورد حمله‌ی هکرهای پاکستانی قرار گرفتند.

- در سپتامبر ۲۰۱۰م.، تأسیسات اتمی کشورمان توسط ویروس استاکس نت مورد هجوم قرار گرفت. این ویروس یکی از پیشرفته‌ترین ویروس‌های رایانه‌ای بود و برگ جدیدی را در مبارزه‌های سایبری گشود.

- در سال ۲۰۱۰م. دوباره دولت انگلیس اعلام کرد که در هر ماه، هدف بیش از ۱۰۰۰ حمله‌ی سایبری قرار می‌گیرد.

- در ژوئیه‌ی ۲۰۱۱م. تارنمای شرکت ارتباطاتی (SK) کره جنوبی هک شد و اطلاعات شماره تلفن، پست‌های الکترونیک و آدرس منزل ۳۵ میلیون نفر دزدیده شد.

- در اکتبر ۲۰۱۱م.، دولت آمریکا پذیرفت که کنترل هواپیمای جاسوسی خود را در یک حمله‌ی سایبری از سوی ایران از دست داده است.

- در سال ۲۰۱۲م. بیان شد که هند اطلاعات کمیسیون دوجانبه‌ی اقتصادی بین چین و آمریکا را هک کرده است. گویا اطلاعات هک شده شامل تبادلات پست‌های الکترونیک بین اعضای کمیسیون دوجانبه بوده است.

مهم‌ترین مسئله در این بین، این است که حملات سایبری برای مهاجم ارزان تمام شده ولی دفاع در برابر این حملات بسیار گران تمام می‌شود .

تلاش‌ها برای پیشگیری

شاید اولین سازمان بین‌المللی سازمان همکاری‌های شانگ‌های باشد که جنگ مجازی را به عنوان عامل مخرب برای اخلاق، معنویت و فرهنگ از سوی مهاجمان تعریف کرده است. در سپتامبر ۲۰۱۱م. کشورهای عضو پیشنهاد تدوین شاخص‌های بین‌المللی

برای یک سند جامع امنیت اطلاعاتی را به دبیر کل سازمان ملل ارائه دادند .این طرح از سوی کشورهای غربی حمایت نگردید. رویکرد کشورهای غربی بیشتر بر جنبه‌های اقتصادی متمرکز بود .

در حال حاضر پروژه‌ای توسط دکتر (Alexander Merezhko)استاد حقوق بین‌الملل در حال تدوین برای ارائه به سازمان ملل است. طبق این سند جنگ مجازی به معنای استفاده از اینترنت و فناوری‌های وابسته به آن توسط یک دولت، برضد منافع اقتصادی، سیاسی، فناوری و اطلاعاتی یک حاکمیت دیگر است. وی بیان می‌دارد که اینترنت میراث مشترک بشری است و باید از جنبه‌های نظامی مصون بماند.

جنگ در فضای مجازی تا حد زیادی به ضعف سیستم دفاعی مورد حمله قرار گرفته بستگی دارد. این جنگ ابهام‌هایی همچنین در مورد شخص حمله کننده دارد که به واقع چه کسی حمله را آغاز می‌کند. همان‌گونه که شبکه‌های رایانه‌ای به عنوان مهم‌ترین عامل برای قدرت اقتصادی و حتی نظامی کشورها تبدیل شده‌اند، همچنین آن‌ها به مأمنی برای تهدیدهای بالقوه نیز تبدیل شده‌اند. از طرفی فضای مجازی می‌تواند به عنوان یک کمک برای حملات نظامی فیزیکی در نظر گرفته شود.

مشکل بزرگ این است که شبکه‌ها به هم متصل هستند. اگر یک رایانه‌ی خانگی هم در یک کشور سیستم دفاعی ضعیفی داشته باشد، ممکن است از راه این رایانه بتوان به سایر رایانه‌های آن کشور هم دسترسی پیدا کرد. امروزه میزان استفاده از رایانه‌های شخصی با سرعت زیادی در حال پیشرفت است. در جنگ واقعی همه چیز قابل پیش‌بینی است. میزان خسارتی که یک بمب می‌تواند وارد کند و خسارت‌های احتمالی مالی و جانی، اما در جنگ مجازی هیچ خسارتی قابل پیش‌بینی نیست(*).

پی‌نوشت‌ها :

[1] -European Network and Information Security Agency
[2] -flame
[3] -Sabotage

:منابع

1. Russia Toda, 26 Jan. 2012, "US Launched Cyber Attacks on Other Nations," https://rt.com/usa/news/us-attacks-cyber-war-615/
2. Pentagon Bill To Fix Cyber Attacks: $100M. CBS News. Retrieved on 2011-11-08.
3. Gorman, Siobhan. (2010-06-04) WSJ: U.S. Backs Talks on Cyber Warfare. Online.wsj.com. Retrieved on 2011-11-08.
4. a b Clarke, Richard A. Cyber War, HarperCollins (2010)

سعید واحدی‌فرد؛ کارشناس ارشد علوم ارتباطات*

آدرس لینک مربوطه http://jangnarm.com/index.aspx?siteid=51&pageid=21019&newsview=14994 :