جنگ نامتقارن[1]

محمدرضا رزمخواه

مقدمه

برای نخستین بار و بطور رسمی مفهوم جنگ نا متقارن در گزارش بررسی دفاعی چهارساله آمریکا در سال ۱۹۷۷ مورد استفاده قرار گرفت.از مجموع تعریف های ارائه شده برای جنگ نا متقارن به چند عنصر اصلی از جمله بهره گیری از نقاط ضعف و آسیب پذیری دشمن , استفاده از فناوری های پیشرفته و غیر قابل انتظار , بهره گیری از روش های مبتکرانه , تضعیف اراده ی دشمن برتر , تاکید بر تایید نامتناسب را می توان اشاره نمود .

ستاد مشترک آمریکا از جنگ نا متقارن تعریفی اینگونه دارد "به کارگیری رویکردهای غیر قابل پیش بینی یا غیر متعارف برای خنثی نمودن یا تضعیف قوای دشمن و در عین حال, بهره برداری از نقاط آسیب پذیر او از طریق فناوری های غیر قابل انتظار یا روش های مبتکرانه"

جنگ نامتقارن را می توان در ابعاد هسته ای , شیمیایی , بیولوژیکی, الکترومغناطیسی , سایبریک و ... مورد مطالعه قرار داده و یا آنرا بکار بست. در این مقاله به بعد سایبریک آن پرداخته شده است .

۲

Cyber عبارت است از کلمات مرتبط با رایانه، فناوری اطلاعات، اینترنت و حقایقی واقعی است که برای بیان مفاهیمی مربوط به آینده است.

---

[1] Asymmetrical warfare

1- oxford English dictionary fifth edition 2002

همگام با آماده شدن و تجهیز قدرتهای بزرگ , انقلابی بی سابقه در حال شکل گیری است و آن چیزی جز انقلاب اطلاعات نیست . توسعه وسایل ارتباطات اینترنتی، این انقلاب را در سراسر جهان گسترانیده و محیطی تازه به وجود آورده است برای حفظ بقا، در چنین محیطی , ضروریست تا شناخت کافی از تهدیدها , فرصت ها و امکانات بالقوه داشت .

به کار گیری رایانه های نسل سوم و چهارم ماهیت اساسی راهبرد نظامی, سازمان ها و ساختارهای نظامی , دکترین و استراتژی ها را تغییر داده است .

به نظر می رسد استفاده از قدرت آتش وسیع بهمراه ارتش مکانیزه و هواپیماهای بمب افکن قول پیکر , دیگر مربوط به گذشته باشد . اکنون با جنگ رایانه ای، شکست یا پیروزی حاصل انبوه تجهیزات و لشکر نبوده، بلکه بستگی به اطلاعات و دانش برتر دارد. کسانی که در این زمینه به موفقیت هایی نایل آیند به مزایایی دست خواهند یافت که نتایج آن کمتر از داشتن بمب اتم نیست .

دستیابی به توانمندی های جنگ سایبریک , به حمله کننده، قدرت تخریب جبران ناپذیری حتی بدون شلیک یک گلوله می دهد . توان فوق العاده که یک کشور از این طریق کسب می کند می تواند دشمن را همچون یک بمب اتم منفعل و در عین حال ارتش سازمان یافته و منظمی هم نداشته باشد .

در جنگ های متعارف امروزی همچون جنگ های خلیج فارس، بالکان , افغانستان و عراق، همواره حمله های پیشگیرانه و ویران کننده بر علیه مراکز فرماندهی , سایت ها و سامانه های رادار دفاع هوایی , مراکز ارتباطی فرماندهی وکنترل (C4I) انجام و متعاقب آن یورش به کارخانجات برق, دپوهای مهمات، سوخت و مراکز اصلی نیروهای آفندی نظامی کشورهای هدف آغاز می گردید . یکی از اهداف اولیه این نوع

حملات , ایجاد رعب و وحشت در میان فرماندهان طرف مقابل و از هم گسیختگی سازمانی به منظور انهدام ماشین جنگی آنان است .

در جنگ سایبریک نیز یک چنین سناریو با اولویت بندی مشابه طرح ریزی می شود، تا با زمین گیر ساختن دشمن بدون هرگونه برخورد فیزیکی و تحمیل خسارت پیروزی حاصل شود .

از این رو، در اینگونه جنگ ها ,هدف نهایی فلج کردن و از کار انداختن
سامانه ها و سازمان های معمول نظامی کشور هدف بوده، تا نتوانند ادامه فعالیت بدهند.

۲– بازتاب های جنگ سایبریک

در یک حمله ی سایبریک به کشوری که اکثر جمعیت , وسایل حمل و نقل, مراکز دولتی و تجاری در چند شهر عمده گرد هم آمده است , چنانچه حمله متوجه مغز شبکه گردد , نتایج زیر حاصل می گردد که اثری همچون یک بمب اتم دارد.

۱-۲- برق قطع می شود , لذا با قطع برق کلیه ی زیرساخت های برقی کشور بطور کل فلج شده , سامانه حمل و نقل, آسانسورها , سامانه گرم کننده و خنک کننده و۰۰۰ از کار خواهد افتاد .

۲- ۲- سامانه مخابراتی مختل و یا قطع می شود . در این حالت تلویزیون, رادیو , تلفن , سامانه های کنترل ترافیک و ایستگاه های هواشناسی قادر به فعالیت نخواهند بود .

۳-۲- سامانه آبرسانی و توزیع مواد غذایی دچار اختلال می شود .

۴-۲- موسسات کلیدی همچون بانک ها , مراکز پزشکی , سوپرمارکت ها و ۰۰۰ دچار اشکال می شوند .

۲-۵- سامانه های اورژانس و درمان غیر فعال خواهند شد و با توجه به اوضاع آشفته و غیر فعال بودن پلیس, جامعه دچار هرج و مرج می گردد .
۲-۶- بخش اعظمی از سازمان ها و تشکیلات نظامی نیز فلج خواهد شد , تأخیر در عکس العمل به موقع توانمندی های نیروی هوایی , رادارهای دفاع هوایی و سامانه های ردیاب در حالی که قدرت تحرک و طرح های گسترش نیز نابود شده اند یا قابل دسترس نمی باشند و سامانه لجستیک نیز غیر قابل بهره برداری می گردد.
۲-۷- بخش اعظمی از سامانه حمل و نقل فلج شده و غیر قابل حرکت می گردد . ترافیک ایجاد شده در چنین شرایطی در مقایسه با ترافیک عادی شهرهای بزرگ قابل کنترل نخواهد بود . تصور شهرهای بزرگی چون توکیو, لندن، نیویورک و ... بدون مترو , سامانه حمل و نقل , خدمات فرودگاهی و هواپیما , قطار , شبکه کنترل ترافیک و ۰۰۰ قابل تحمل نخواهد بود .

شوک ایجاد شده توسط این تهاجم ها باعث هرج و مرج میان مردم شده و برمیزان خرابی ها خواهد افزود , جامعه از کار و فعالیت باز خواهد ایستاد و قانون جنگل حکم فرما خواهد شد . هر قدر شهر صنعتی تر باشد, میزان خرابی ها و اثر جنگ سایبریک بیشتر خواهد بود .

۳- چگونگی عملکرد جنگ سایبریک

صاحب نظران اطلاعاتی معتقدند که در عصر اینترنت , هنگامی که سرعت ارتباطات در سراسر دنیا به نانو ثانیه می رسد, گروه های خرابکار در جنگ سایبریک برنده خواهند بود . خرابکاران با بکارگیری نرم افزارهای رمز شده , ارتباطات خود را مخفی نگاه می دارند .

۳-۱- هکرها (HACKERS)

خرابکاران با بکارگیری رایانه های هکر (نفوذ کننده) قادرند به شبکه های دولتی کشورهای هدف وارد شده و اهداف مورد نظر خود را دنبال کنند .

امروزه برنامه های رایگان هکر بسیاری در شبکه اینترنت ارائه می گردد که می توانند خطر آفرین باشند . از طرفی تا پایان سال ۲۰۰۵ استفاده کنندگان از شبکه ی اینترنت به یک میلیارد نفر خواهد رسید . قابل ذکر است که در سال ۱۹۹۵ حدود ۲۵۰/۰۰۰ هکر به رایانه های پنتاگون نفوذ کرده و ۶۵ در صد آنها وارد شبکه شده اند.

تحلیل گران امور معتقدند که این گونه جرائم نامرعی بوده , نه تنها تعقیب کردن آنها مشکل است , بلکه مشخص کردن اینکه چه کسی آنرا انجام داده و آیا اینکه اصلا" رایانه ای هک شده (مورد هجوم قرار گرفته) یا خیر نیز قابل تشخیص نیست .

۳-۲-کراکرها (CRACKERS)

برخی از هکرهای پیچیده که کراکر نام دارند , قادر هستند تا دولت ها و شرکت های زنجیره ای را دچار کابوس مالی کنند . قابل ذکر است که همه ساله حدود ۱۰-۹ میلیارد دلار از همین طریق به سرقت می رود . گزارش دیگری حاکی از آن است که وزارت دفاع آمریکا روزانه حدود ۱۰۰-۸۰ بار مورد حمله سایبریک قرار می گیرد که فقط ۱۰ مورد آن قابل تعقیب است .

در همین رابطه برخی از هکرها که ملیت آمریکایی , انگلیسی و روسی داشته اند , توانسته اند تعدادی از پرونده های طبقه بندی شده را به سرقت ببرند . آنها قادرند ارتباط بین سایت ها را قطع و در ارتباطات

GPS که کنترل کننده سامانه سلاح های موشکی و پیشرفته هدایت شونده هستند , اختلال ایجاد نمایند .

کوشنر (Ckushner) نویسنده ی کتاب " *تروریسم در آمریکا* " می گوید : در جنگ سایبریک , صنایع غذایی بسیار آسیب پذیرند . خرابکاران قادرند فرمول مواد غذایی را تغییر داده , آنها را مسموم نموده و بخش اعظمی از جامعه را دچار مشکل کنند .

در جنگ سایبریک , هکرها قادرند رمزهای رایانه ها را تغییر داده , هواپیماها را به پرواز در آورند , کنترل سامانه های ناوبری را به عهده گرفته و آنها را به مقصد دلخواه هدایت و یا اینکه آنها را وادار به سقوط کنند.

از طرفی کشورهای پیشرفته در اقصی نقاط جهان در حال تبیین راهبردی مناسب در جهت کم و کیف جنگ سایبریک هستند، تا ضمن کسب توانایی, نفوذ در شبکه ی فرماندهی و کنترل , لجستیک , حمل و نقل و رادارهای اخطار اولیه و سایر عملیات نظامی دشمن , خود نیز از نفوذ عملیات مشابه توسط دشمن در امان باشند .

البته برای کشورهای کوچک تر که توانایی مقابله با قدرت نظامی متعارف همسایگان بزرگ تر را ندارند به مراتب سهل تر است تا از طریق جنگ سایبریک به قدرت استراتژیک دست یابند .

گستردگی عملیات جنگ سایبریک , سازمان های اطلاعاتی کشورهای صنعتی و به ویژه آمریکا را باکمبود بودجه و متخصص جهت کنترل و مقابله با هکرها روبرو کرده است .

کشورهایی چون آمریکا و اعضای پیمان ناتو که توانایی به کارگیری جنگ سایبریک را در کنار عملیات نظامی دارند و قادرند تسلط اطلاعاتی

برروی منطقه ی نبرد ایجاد کنند , کشورهایی هستند که در مقابل جنگ سایبریک نامحدود , آسیب پذیرتر هستند .

۴– گروه بندی جنگ سایبریک

۴–۱– جنگ سایبریک در کنار عملیات نظامی

هنگامی که تشکیلات نظامی درگیر یک نبرد خصمانه است , مساله اصلی کسب برتری اطلاعات و یا تسلط اطلاعاتی در فضای جنگ است . این امر با مختل کردن سامانه دفاع هوایی دشمن , بلوکه و یا انهدام رادارها و موارد مشابه صورت می گیرد . برابر نظریه ی کلازویتز , هدف ایجاد و افزایش " سردرگمی در جنگ[1] " برای دشمن و کاهش آن برای نیروهای خودی است . این امر از طریق حملات مستقیم به شبکه ی ارتباطی و پردازش اطلاعات دشمن و یا از طریق حمله به سامانه های داخلی صورت می گیرد . تمرکز در این روش بستگی به اهداف سایبریک نظامی دارد .

جنگ سایبریک محدود

در این مرحله , هدف و سلاح حمله محیط زیربنایی اطلاعات با عملیات واقعی محدود در جهت همراهی حمله است . حمله اطلاعاتی معمولا" از طریق تداخل بین دشمن و متحدان اوصورت می گیرد . روش دیگر این است که عوامل درونی و یا جاسوسان, نرم افزار مورد نظر را به طور مستقیم" وارد شبکه ی دشمن کنند .

با کاهش اثربخشی سامانه های ارتباطی دشمن و جلوگیری از بهره گیری عملیات نظامی که متکی به شبکه ی ارتباطی است , نیروهای

1- fog of war

دشمن ناگزیر به استفاده از روش های قدیمی تر جهت عملیات نظامی شده و لذا باعث افزایش آسیب پذیری آنها خواهد شد .
جنگ سایبریک محدود معمولا" جهت کند کردن آمادگی های دشمن برای عملیات نظامی طرح ریزی می گردد .

جنگ سایبریک نامحدود

این نوع جنگ برعلیه منابع حیاتی کشور هدف از جمله : نیروگاه برق , حمل و نقل , شبکه بانکی , آب , ارتباطات , خدمات اضطراری، اورژانس و اطلاعات طرح ریزی می گردد. این نوع جنگ از مرزها عبور کرده و پیامدهای آنی و تأخیری خواهد داشت .

این نوع حمله باعث تباهی جامعه , اقتصاد و از بین رفتن جان انسان ها می گردد . کندی در خدمات اورژانس در شهرهای بزرگ نه تنها باعث مرگ نیازمندان به خدمات مربوطه می گردد , بلکه باعث بی اعتمادی مسوولین دولتی در ارائه خدمات مورد نیاز به مردم خواهد شد. با قطعی شدن حمله به سایر منابع همچون ارتباطات , حمل و نقل و آب , ترس ایجاد شده و عدم اعتماد حاصله در بین مردم باعث از هم گسیختگی جامعه می گردد . حمله بر علیه منابع مالی , حجم تجارت را کاهش داده و اطمینان مردم را در این زمینه پایین می آورد که از جمله حساب های کارکنان دولت , سرمایه گذاری ها و حساب های پس انداز تحت تأثیر قرار می گیرد .

در صورتی که شبکه های نظامی از کانال مخابرات تجاری استفاده نمایند آنها نیز مورد حمله ی سایبریک در سطوح فرماندهی و کنترل , لجستیک و عملیات نظامی قرار خواهند گرفت .

۵- روش های مقابله با جنگ سایبریک

طرق بسیاری وجود دارد تا میزان آسیب پذیری را در مقابل جنگ سایبریک کاهش داد. اهم این موارد شامل پیش بینی و ارزیابی , اقدامات پیشگیرانه یا بازدارنده , اقدامات دفاعی و اقداماتی به منظور تعدیل خسارت یا بازسازی می باشد . برخی از این اقدامات عبارتند از :

- تهیه لیستی جامع از کلیه ی موارد آسیب پذیر سازمان های عمده ی دولتی و بازرگانی
- ابداع هرگونه اقدام متقابل جهت دفاع و حفاظت موارد آسیب پذیر از جمله :
  - عدم اتصال شبکه های داخلی به شبکه جهانی اینترنت
  - جدا سازی شبکه های رایانه ای نظامی از غیر نظامی
  - ایجاد شبکه کنترل غیر رایانه ای رزرو
- بسیج بهترین و قابل ترین نیروهای انسانی کارآمد جهت تهیه طرح های کلان برای تمامی پیشامدهای احتمالی (مدیریت بحران)
- در نهایت اینکه مقایسه ی بهترین و ایده آل ترین اقدام متقابل بر علیه فناوری ها , منابع و بودجه

۶- نتیجه :

با توجه به نظریه کلازویتز که جنگ به طریق دیگر ادامه سیاست است[۱] , در هر دو زمینه ی جنگ کلاسیک و نا متقارن (جنگ سایبریک) صادق است . هوشیاری از درگیری های فزاینده ی سیاسی , شناسایی و تجزیه و تحلیل گسترش توانمندی های جنگ سایبریک و شناسایی و ارزیابی، پیش در آمدهای حمله , همگی فراهم

[۱] کتاب هنر جنگ

کننده ی اخطارهایی از شروع حملات سایبریک است . با این حال , تشخیص عوامل یک حمله ی واقعی از یک حمله تصادفی سایبریک نه ساده است و نه در کوتاه زمان قابل تشخیص می باشد . در جنگ سایبریک اقدامات پیشگیرانه یا بازدارنده بسیار مشکل است . از آنجا که وابستگی کشورهای پیشرفته به سامانه های رایانه ای باعث آسیب پذیری بیشتر آنها در مقابل جنگ های سایبریک می گردد و از طرفی , فعالیت در این زمینه نیز نیاز به سرمایه گذاری و فناوری قابل توجهی ندارد , از این رو به نظر می رسد , دستیابی به مقوله یاد شده که می تواند در چارچوب جنگ های نا متقارن قرار گیرد , کشور ج.ا.ا را در جهت تقویت بنیه دفاعی و کسب بیشتر اقتدار ملی در رویارویی با استکبارجهانی یاری نماید.

۷- مراجع

1)Tong-Chin,Rhee,(2003),Are we preparing for one?, www.hk.co.kr/14-1

2)Waller,Michael,(2000),PLA Revises the Art of War www.findarticles.com/cf-o/m1567/15-14/66.html

3)Maier,Timothy,(1999),Is US Ready fo Cyber Warfare? , www.findarticles.com/cf-o/m1571/13-

15/54.html 4)Shimeal,Timothy,(2001),Countering Cyber War,
www.nato.int/docu/review/2001/0104.toc.htmh
۵-, کنت مکنزی , ترجمه حیدری عبدالمجید , جنگ نا متقارن، تهران , دافوس سپاه , دوره عالی جنگ , ۱۳۸۲