سایبرنتیک و جنگ نرم، پنجمین میدان نبرد

امیر هوشنگ خادم دقیق[۱]، مازیار مستعد[۲]

[۱] کارشناسی ارشد، نیروی هوایی ارتش ج.ا.ا، تهران، ایران

[۲] کارشناس، نیروی هوایی ارتش ج.ا.ا، تهران، ایران

maziar_mostaed@yahoo.com

چکیده :

هیچ انسانی بدون امنیت نمی‌تواند به ادامه‌ی حیات خود امیدوار باشد؛ چه در دنیای واقعی چه در دنیای مجازی. موضوع امنیت یکی از اصلی‌ترین شاخصه‌ها و نیازهای بشری است و این خصوصیات، امروزه در دنیای سایبر نیز محسوس و ملموس است. اخبار و آمار امنیتی شدن فضای سایبر مدت‌هاست که جزو اخبار اول رسانه‌ها شده و بسیاری نیز بر این عقیده‌اند که این آغازی است بر "جنگ سایبر" بین دولت‌ها و شاید در گستره "جنگ جهانی سوم."در این مقاله سعی نموده‌ایم به ابعاد گوناگون این بحث مهم ازمنظر جنگ نرم با عنوان پنجمین میدان نبرد بپردازیم.

واژگان کلیدی:

جنگ اطلاعاتی، جنگ سایبری، انواع نفوذگران در جنگ سایبری، انواع حملات نفوذگران، نقاط ضعف دفاع سایبری، اقدامات برخی از کشورها پیرامون سایبرنتیک ، تهدیدشناسی، تهدید نرم، ویژگی‌ها و سطوح قدرت نرم.

۱- مقدمه:

سایبر بخشی از کلمه Cybernetics است . کلمه Cybernetics را اولین بار نوربر وینر [1]به‌کار برد. او در تعریف این کلمه گفته‌است: "ما تصمیم گرفته‌ایم کلیت مطالعات نظری کنترل و ارتباطات در ماشین و موجودات زنده را سایبرنتیکس بنامیم." سایبرنتیکس ریشه در کلمه لاتین "Gubernetes " دارد. این کلمه به‌معنی کنترل رفتارها به‌منظور هدایت، اعمال قدرت حاکمیت، قانونمند کردن، تحت سلطه قراردادن، مهارکردن، و فرماندهی است. خود این واژه لاتین نیز ریشه در کلمه یونانی Kubernetes-pilot دارد. Pilot به‌معنی حاکم و فرمانده ـ به‌ویژه ناخدای کشتی و خلبان هواپیماست. از طرف دیگر S در Cybernetics نشانگرحضور علم یا مطالعه است . پس در معنای عام علم یا "مطالعه نظام کنترل ارتباطی ـ اطلاعاتی" در موجودات زنده و ماشین را گویند. این کلمه در بعضی از متون، به‌اختصار "فرمان‌شناسی" ترجمه شده-است. محیط سایبر از لحاظ لغوی، محیطی است مجازی وغیرملموس درفضای شبکه‌های بین‌المللی(این شبکه ها از طریق شاهراه‌های اطلاعاتی مثل بستر فیزیکی اینترنت‌به‌هم وصل هستند)که دراین محیط تمام اطلاعات راجع‌به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورهاو به‌طورکلی هرآن‌چه در کره خاکی به-صورت ملموس وجوددارد(درصورنوشته، تصویر، صوت، اسناد) دریک فضای مجازی به‌شکل دیجیتالی وجودداشته و قابل‌استفاده ودر دسترس کاربران بوده واز طریق‌کامپیوتر، اجزای آن وشبکه‌های بین‌المللی به‌هم مرتبط می‌باشند.

"مارک پالمر" از استراتژیست‌های معروف آمریکایی است که از او به‌عنوان یکی از نوآوران سیاست خارجی ایالات متحده نام می‌برند. پالمر در دولت‌های نیکسون، کارتر، ریگان و بوش در وزارت خارجه ایالات متحده مشغول بوده و اکنون علاوه‌براین‌که مدیر دپارتمان تحقیقاتی مرکز سیاست خارجی سابان در مؤسسه‌ی "بروکینگز" می‌باشد، عضو کمیته‌ی خطر جاری است که در پی تحولات پیش‌آمده پس از یازده سپتامبر ۲۰۰۱ گزارشی تحت عنوان "ایران- آمریکا، رهیافت جدید" را به نگارش درآورد. کمیته‌ی خطر جاری در اوج جنگ سرد و در دهه ۱۹۷۰ میلادی و با مشارکت اساتید برجسته‌ی علوم سیاسی و مدیران سابقه‌دار سازمان سیا و پنتاگون تأسیس شد و یکی از موفقیت‌آمیزترین اقدامات در جریان رقابت دو ابرقدرت شرق و غرب، طراحی و اجرای مراحل مختلف سناریوی فروپاشی ابرقدرت شرق از طریق "جنگ نرم" (Soft War) در سال‌های پایانی دهه‌ی ۱۹۸۰ بود.

مارک پالمر نویسنده‌ی گزارش "ایران- آمریکا، رهیافت جدید" در استدلال خود، صراحتاً با ایده‌ی تهاجم نظامی علیه جمهوری اسلامی ایران مخالفت کرده و اعلام نموده ایران به‌لحاظ وسعت سرزمینی، کمیت جمعیت، کیفیت نیروی انسانی، امکانات نظامی، منابع طبیعی سرشار و موقعیت جغرافیایی ممتاز در منطقه‌ی خاورمیانه و نظام بین‌الملل به‌قدرتی کم‌مانند تبدیل شده که دیگر نمی‌توان با یورش نظامی و جنگ سخت آن را سرنگون کرد. تنها راه مبارزه با نظام جمهوری اسلامی، پیگیری مکانیسم‌های جنگ-نرم و استفاده از تکنیک‌های عملیات روانی تبلیغاتی با استفاده از سه تاکتیک دکترین "مهار"، "نبرد رسانه‌ای" و "ساماندهی و پشتیبانی از نافرمانی مدنی" است.

درپایان این گزارش با منتفی دانستن هرگونه گفت‌وگو و مذاکره‌ی مستقیم با مقامات ایرانی آمده است: "گفتگو فقط حکومت ایران را تقویت و محکم می‌کند. باید از طریق انزوا و تقویت مخالفان داخل و خارج حکومت در جهت تغییر این رژیم تلاش کرد."

۲- جنگ اطلاعاتی:

جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است.این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد. مارتین لیبیکی، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی ایالات متحده، در کتاب «جنگ اطلاعاتی چیست؟» می‌نویسد «تلاش برای درک مفهوم جنگ اطلاعاتی مانند این است که چند نفر نابینا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست. جنگ اطلاعاتی نیز شامل بخش‌های مختلف و متعددی می‌باشد.» تلاش برای برخورداری از نگرش جامعه نگرانه در تعریف جنگ اطلاعات نکته‌ایست که باید حتماً به آن توجه شود.مگان برنز در سال ۱۹۹۹ با نگرشی کلی تعریف زیر را ارائه می‌دهد «جنگ اطلاعاتی طبقه یا مجموع تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و جلوگیری از افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر

[1] - Norbert Wiener

دشمنان خود به مزیتی چشم‌گیر دست یافته و آن را حفظ می‌کند.»

مارتین لیبیکی ضمن وفادارماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به‌شرح زیر نام-می‌برد:

- جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن است.
- جنگ برپایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سامانه‌هایی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
- جنگ الکترونیک تکنیک‌های رادیویی، الکترونیک، یا رمزنگاری.
- جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف‌ها، و دشمنان استفاده می‌شود.
- جنگ هکرها که در آن به سامانه‌های رایانه‌ای حمله می‌شود.
- جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
- جنگ سایبر: ترکیبی از همه موارد شش گانه بالا.

۳- جنگ سایبری (تعاریف)

با نگرش به مفاهیم مطروحه در بخش‌های قبل، جنگ سایبری به-احتمال قوی از جدی‌ترین چالش‌های امنیتی است که از طریق فضای مجازی به دولت‌ها تحمیل می‌شود. مشابه با ابزارهای جنگ متعارف؛ از فناوری سایبری نیز می‌توان برای حمله به تشکیلات دولتی، زیرساخت‌های ملی انرژی و تضعیف روحیه عمومی بهره جست.

موسسه چتم هاوس در گزارشی با عنوان "جنگ سایبری" به‌قلم چهار تن از نویسندگان به نام‌های "پل کورنیش"، "دیوید لیوینگستون"، "دیو کلمنته" و "کلر یورک" به بررسی ابعاد مختلف جنگ سایبری پرداخته است :

در سال‌های اخیر، دولت‌ها و سازمان‌های بین‌المللی بر امنیت سایبری تمرکز بیشتری نموده‌اند و از شرایط اضطراری آن کاملاً اطلاع دارند. در انگلیس، امنیت سایبری عمدتاً در "راهبرد امنیت ملی" و" نشریه دفاع و امنیت راهبردی" که در اکتبر ۲۰۱۰ به-چاپ رسیده، مطرح شده است.

بارزترین ویژگی جنگ سایبری تحول سریع تهدیدات است، نوع اقدامات تهاجمی و ویژگی‌های آن به‌اندازه خود بازیگران اهمیت دارد. برای مثال، فعالیت‌های سایبری گروه‌های تروریستی، جاسوسان و جنایتکاران سازمان‌یافته می‌توانند مخرب بوده و تهاجمی باشند اما ضرورتاً از مصادیق جنگ سایبری تلقی نمی‌شوند.جنگ سایبری می‌تواند از مصادیق و جلوه‌های"جنگ نامتقارن"– یعنی، نبردی که در آن سامانه‌های ضعیف‌تر با کشف نقاط آسیب‌پذیر سامانه‌های قدرتمند در پی یافتن راهکارهایی مبتکرانه به‌منظور به‌حداکثر رساندن برتری‌های خودی و بهره-برداری از این نقاط آسیب‌پذیر هستند- باشد.درجنگ نامتقارن اغلب تاثیرات (نظامی یا سیاسی) نسبت به میزان نیروی به‌کار-گرفته شده عظیم است .

همانگونه که مطرح شد بارزترین ویژگی جنگ سایبری (امنیت سایبری به‌طورعام)، تحول سریع تهدیدات است. این تغییرات می‌توانند آن‌قدر ناگهانی و غیرمنتظره باشند که از همان ابتدا دور تسلسل عمل و عکس‌العمل در راهبرد سنتی را از حرکت بیاندازند. جنگ سایبری مدل بدون درد و خونریزی جنگ است، این بحث جذاب اما خطرناک مطرح است که جنگ سایبری می‌تواند مدل"بدون‌درد" و"بدون‌خونریزی" جنگ باشد که البته نتایج مهمی را درپی خواهدداشت. پیروزی و شکست در فضای مجازی چندان قابل‌تفکیک از یکدیگر نیست.در جایی که عوامل ایدئولوژیکی، مذهبی، اقتصادی و نظامی به‌دلایل مختلف و در مقاطع زمانی متفاوت به مقابله با یکدیگر برمی‌خیزند، این مفاهیم جذابیت زیادی نخواهند داشت. این مسئله به یک محیط رزمی نامتقارن و بی‌نظم منجر می‌شود که معلوم نیست در آن‌جا بتوان از معیارهای مشترک اخلاقی، هنجاری و ارزشی بهره-گرفت.لازمست علاوه‌بر تشریح عمل‌کرد مهاجمان مجازی و واکنش دولت‌های مدافع و نیز تحلیل نتایج، روش‌ها و ابزارهای جنگ‌سایبری، مشخصات اصلی جنگ سایبری را به‌عنوان یک پدیده راهبردی برشمرد.

از این رو، تعریف زیر نیز برای جنگ سایبری پیشنهاد می‌شود:

- جنگ سایبری می‌تواند بین دولتها یا از برخی جهات حتی بین بازیگران غیردولتی اتفاق افتد. در این جنگ، هدایت دقیق و مناسب نیروها بسیار دشوار است، هدف می‌تواند نظامی، صنعتی، غیرنظامی یا حتی فضای سروری باشد که مطمئناً به مشتریان بسیاری خدمات ارائه می‌دهد.

بارزترین ویژگی‌های جنگ سایبری عبارتند از:

- جنگ سایبری به بازیگران این امکان را می‌دهد که بدون توسل به جنگ مسلحانه، به اهداف سیاسی و راهبردی خود دست یابند.
- فضای مجازی قدرت غیرواقعی به بازیگران کوچک و کم‌اهمیت می‌دهد.
- با استفاده از آدرس IP اشتباه، سرورهای خارجی و اسامی مستعار، مهاجمان می‌توانند در عین ناشناس بودن و مصونیت نسبی، برای مدت کوتاهی فعالیت کنند.
- در فضای مجازی، مرز بین نظامی و غیرنظامی و نیز فیزیکی و مجازی چندان روشن و شفاف نیست.
- در کنار سایر میادین سنتی نبرد مثل زمین، هوا، دریا و فضا، باید فضای مجازی را "پنجمین میدان نبرد" دانست. جنگ سایبری از اجزای جدید این محیط چندبعدی است اما کاملاً جدا از آن در نظر گرفته نمی‌شود.
- در فضای مجازی، اقدامات شبه‌جنگی به‌احتمال زیاد همراه با سایر اشکال زور و منازعه رخ می‌دهد. اما، روش‌ها و ابزارهای جنگ سایبری قطعاً متفاوت از سایر جنگ‌ها خواهد بود.

۴-انواع نفوذگران در جنگ سایبر:

همان‌گونه که مطرح گردید جنگ سایبری به‌نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند.

انواع نفوذ گران در جنگ سایبر به‌شرح ذیل می‌باشند :

- گروه نفوذگران کلاه سفید(White hat hackers) :

هر کسی که بتواند ازسد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند.هکرهای کلاه سفید متخصصین شبکه‌ای هستند که حفره‌های امنیتی شبکه را پیدا می‌کنند و به مسوولان گزارش می‌دهند.

- گروه نفوذگران کلاه سیاه(Black hat hackers):

اشخاصی هستند که وارد کامپیوتر قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش‌کردن ویروس و غیره می‌پردازند.

- گروه نفوذگران کلاه خاکستری(Gray hat hackers):

اشخاصی هستند که حد وسط دو تعریف بالا می‌شوند.

- گروه نفوذگران کلاه صورتی(Pink hat hackers):

این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

۵- انواع حملات نفوذگران :

- شنود یا Interception

در این روش نفوذگر می‌تواند به شکل مخفیانه از اطلاعات نسخه برداری کند.

- تغییر اطلاعات یا Modification

در این روش نفوذگر به‌دست‌کاری و تغییر اطلاعات می‌پردازد.

- افزودن اطلاعات یا Fabrication

در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

- وقفه یا Interruption

در این روش نوع نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

۶-اقدامات برخی از کشورها پیرامون سایبرنتیک:

- **روسیه**

سران روسیه اهمیت ویژه‌ای برای جنگ سایبر قائل هستند به‌گونه‌ای که در رتبه‌بندی از نظر اهمیت، جنگ سایبر را دقیقا بعد از جنگ هسته‌ای قرار می‌دهند. در سال ۱۹۹۵ یکی از فرماندهان روسی در کنفرانس مشترک روسیه – آمریکا درباره امنیت ملی در دوران پس از جنگ سرد اظهار داشت «از دیدگاه نظامی، ما استفاده دشمنان از جنگ اطلاعاتی علیه کشور یا نیروهای مسلح روسیه را به عنوان یک مرحله غیر نظامی درگیری تلقی نمی‌کنیم. با توجه به ابعاد و عواقب فاجعه‌آمیز استفاده از جنگ اطلاعاتی راهبردی علیه نظام اقتصادی ملی، نظام فرماندهی و کنترل، و به طورکلی علیه توانمندی‌های دفاعی و رزمی روسیه ، ما این حق را برای خود محفوظ می‌دانیم که در برابر ابزارها و نیروهای مهاجم اطلاعاتی و در مرحله بعد علیه خود کشور مهاجم از سلاح هسته‌ای استفاده کنیم.»

- **چین**

امروزه چین تعاریف و مفاهیم جدیدی را در واژگان نظامی وارد

کرده‌است. در سال‌های اخیر، چین در زمینه استفاده از فناوری-های نوین و نیز تغییرات فراوان درسامانه آموزش، یک انقلاب نظامی واقعی در فضای سایبر را تجربه می‌کند. فعالیت‌های چین به‌قدری پیشرفت کرده‌است که موجب نگرانی مقامات آمریکایی گردیده‌است.

علی‌رغم اینکه فعالیت‌های چین محدود به‌ترجمه اسناد و مدارک تهیه شده توسط آمریکایی‌هاست اما برخی دیدگاه‌های چینی را می‌توان در سیاست‌های ارتش چین مشاهده کرد. اساس رویکرد چین به جنگ برپایه فریب، جنگ به سبک دانش و سبک مزیت‌های نامتقارن بر دشمن استوار است.

▪ ایالات متحده آمریکا

آژانس امنیت ملی ایالات متحده : (National Security Agency مشهور به NSA)، یک آژانس دولتی آمریکا است که زیر نظر وزارت دفاع ایالات متحده آمریکا اداره می‌شود. این سازمان در ۴ نوامبر سال ۱۹۵۲ تأسیس شد و وظیفه اصلی آن، نظارت بر مخابرات و فعالیت‌های ماهواره‌ای و کشف رمز در ایالات متحده آمریکا می‌باشد.

این آژانس از اعضای کلیدی جامعه اطلاعاتی ایالات متحده آمریکا است و یکی از محرمانه‌ترین سازمان‌های جاسوسی در جهان به-شمار می‌آید. البته کار این آژانس محدود به جاسوسی ارتباطات است و جاسوسی انسانی را شامل نمی‌شود. همچنین طبق قانون، فعالیت‌های جاسوسی این آژانس محدود به روابط خارجی است اما در برخی مواقع، نظارت‌های داخل مرزی را هم شامل می‌شود. این آژانس از اعضای جامعه اطلاعاتی ایالات متحده آمریکا است و یکی از محرمانه‌ترین سازمان‌های جاسوسی در جهان به‌شمار می‌آید و مرکز آن در ایالت مریلند است.

شنود دائم ارتباطات از راه دور، در سراسر جهان (موبایل، فکس، ای.میل و ارتباطات انفورماتیک) و همچنین دریافت و تحلیل تصاویر ماهواره‌ای، در حوزه‌ی وظایف سازمان امنیت ملی آمریکا (NSA) است. این آژانس که مقرّ آن در فورت مید (مریلند، نزدیک واشنگتن) قرار دارد، قریب به صدهزار نفر کارمند دارد که در مراکز مختلف در آمریکا و ایستگاه‌های شنود مستقر در خارج از این کشور، به‌کار مشغول‌اند. این سازمان از بودجه سالانه‌ای معادل بیش از شانزده میلیارد دلار بهره‌می‌برد. به گفته جان پیک، کارشناس آمریکایی مسائل اطلاعاتی، آژانس امنیت ملی ایالات متحده، حدود ۹۵ درصد ارتباطات از راه‌دور را در سراسر جهان، تحت کنترل دارد. این حجم عظیم اطلاعات به‌وسیله‌ی ابرکامپیوترهای مجهز به نرم‌افزارهای تجزیه و تحلیل، مورد بررسی دقیق قرار می‌گیرد. البته رقم گفته شده از سوی این کارشناس آمریکایی، مورد قبول همهٔ اهل فن نیست، اما می‌توان با اطمینان گفت که توانایی آژانس امنیت ملی آمریکا، در ره‌گیری اطلاعاتی بیش از پنجاه درصد ترافیک جهانی را شامل می‌شود. مدیر این آژانس هنگام یکی از معدود مصاحبه‌هایش با مطبوعات، اعلام کرده بود که او باید هر سه ساعت، اطلاعاتی معادل کل کتابخانه کنگره آمریکا را تحت بررسی داشته باشد. اطلاعات مورد تحلیل سازمان امنیت ملی آمریکا، به‌طور دایم از طریق حدود پنجاه ایستگاه شنود در بیست کشور جهان در سطح پنج قاره دریافت می‌شود. این ایستگاه‌ها وظیفه دارند علامات فرستاده شده از سوی ماهواره‌های مخابراتی را شنود کنند؛ البته عمده این علامات از سوی ماهواره‌های اینتل ست ارسال می‌گردد. مهم‌ترین ایستگاه‌های شنود در کشورهای انگلستان، نیوزیلند، استرالیا و آلمان مستقر هستند.این ایستگاه‌های ره‌گیری علامات ماهواره‌ای، اطلاعات را دریافت می‌کنند؛ خواه از طریق ره‌گیری مستقیم امواج فرستاده شده از سوی ماهواره، یا از طریق دریافت علامات ماهواره‌های ویژه جمع‌آوری اطلاعات در فضا. این ماهواره‌های ره‌گیری که به نام‌های «مرکوری»، «ترومپت»، یا «مانتور» شناخته می‌شوند، همچنین قادر به ره‌گیری امواج رادیوالکتریک از مبدأ زمین هم هستند. برای انجام دقیق مأموریت، برخی از این ماهواره‌ها - مثل ماهواره‌های مرکوری - به آنتن‌هایی مدوّر مجهز هستند که می‌توانند امواج خیلی سبک را منعکس کنند؛ امواجی که سطح‌شان می‌تواند تا سطح یک زمین فوتبال برابر باشد. این آنتن‌های عظیم می‌توانند امواج فرستاده شده از سوی ایستگاه‌های تقویتی تلفن‌های همراه را دریافت کنند. شایع است که ۹ ماهواره از این دست، در اطراف زمین و در ارتفاع ۳۶ هزار کیلومتری از سطح زمین قرار دارند. ۲ ماهواره از این نوع، بر فراز قارهٔ اروپا قرار دارند و اطلاعات دریافتی را به ایستگاه بزرگ منویت هیل در انگلستان ارسال می‌کنند. سازمان امنیت ملی آمریکا روزانه میلیون‌ها ارتباط از راه دور را ره‌گیری می‌کند. تمام ارتباطی که به این ترتیب در چهارگوشه‌ی جهان شنود می‌شوند، به فورت مید

فرستاده شده، در آن‌جا غربال می‌شود؛ تنها بخش کوچکی از اطلاعات ارسالی مورداستفاده بعدی قرار می‌گیرد. اما عملیات غربال چگونه انجام می‌گیرد؟ کامپیوترهایی مجهز به نرم‌افزارهای مخصوص، وظیفهٔ تجزیه و تحلیل و غربال اولیه اطلاعات را برعهده دارند. این کامپیوترها شماره تلفن‌های خاصی را در حافظهٔ خودشان ذخیره کرده‌اند که براساس آن‌ها غربال اولیه را انجام می‌دهند و تنها آن دسته از مکالماتی را که به‌وسیله‌ی این شماره‌ها صورت پذیرفته، نگه می‌دارند. این شماره‌ها عبارتند از: شماره تلفن وزارت‌خانه‌ها، سفارت‌خانه‌ها، روابط‌عمومی سازمان‌های بین‌المللی، سازمان‌های غیر دولتی، شرکت‌های بزرگ فعال در عرصه‌های حساس و مشکوک به رقابت با منافع ملی آمریکا در حوزه‌های مختلف؛ اما گزینش ارتباطات هم‌چنین از طریق شناسایی صدای افراد هم صورت می‌گیرد. میکروچیپ‌های کامپیوترهای کرای (Cray) که شناسایی صداهای آشنا را انجام می‌دهند، در فورت مید و در یک کارخانهٔ ویژه ساخته می‌شوند. کامپیوترهای Cray متعلق به آژانس امنیت ملی آمریکا هماهنگ با بانک داده‌هایشان، قادرند صداهای شخصیت‌های تحت مراقبت مثل شخصیت‌های سیاسی و دیپلماتیک، نظامی، رؤسای شرکت‌ها و ... را شناسایی کنند.

بی‌شک ارتباطات افراد روی شبکه اینترنت نیز تحت کنترل شدید قرار دارد؛ کاملاً محتمل است که آژانس امنیت ملی ایالات متحده با توجه به محتوای روی شبکه، هر لحظه آن‌ها را کنترل کند؛ بر اساس قانون همه شرکت‌های ارائه دهنده خدمات اینترنتی - که اکثرشان آمریکایی هستند - به آژانس امنیت ملی کشورشان اجازه می‌دهند، داده‌های مشتریان‌شان را کنترل کند و همین‌طور ارتباطات اینترنتی‌شان را؛ به علاوه این‌که برخی سایت‌های اینترنتی (اغلب آمریکایی)، گاهی بدون اطلاع صاحبان آن‌ها برای کنترل محتوای کامپیوترهای برخی کاربران اینترنتی، مورد استفاده قرار می‌گیرد. مدتی است که به‌طور مداوم این نجوا به گوش می‌رسد شرکت بزرگ کامپیوتری «مایکروسافت» پیوند نزدیکی با آژانس امنیت ملی آمریکا دارد؛ البته این همکاری‌ها در چارچوب عملیات شنود و ره‌گیری انجام می‌شود. باید بگوییم تنها، آژانس امنیت ملی آمریکا اینترنت را تحت کنترل ندارد؛ بلکه تقریباً تمام سازمان‌های اطلاعاتی آمریکا سرویس‌های ره‌گیری و کنترل خاصّ خودشان را (در مورد اینترنت) دارا هستند؛ این دامنه از CIA تا حتی سرویس اطلاعاتی نیروی دریایی آمریکا را شامل می‌شود.

۷- تهدید شناسی :

در بحث تهدیدشناسی برای رسیدن به هدف مطلوب، اولین مطلب دارای اهمیت، تعریف تهدید است. هر کشوری می‌تواند سه محور را به‌عنوان ارزش‌های حیاتی خود تعریف کند که به مخاطره افتادن آن‌ها به مفهوم از بین رفتن پایه و اساس حاکمیت آن کشور است:

- تمامیت ارضی آن کشور
- ایده‌ها و الگوهای رفتاری جامعه
- حاکمیت مستقر در آن کشور

بنابراین منظور از تهدید، عنصر یا وضعیتی است که یکی از این روش‌های حیاتی را به مخاطره می‌اندازد. اما هدف تهدید چیست؟ هر ویروسی یک هدف دارد؛ هدف ویروس تهدید، مختل کردن و در نهایت از بین بردن امنیت یک جامعه و در نهایت نابودی حاکمیت است. در گذشته از ابزارهای سخت و ادوات نظامی استفاده می‌کردند، اما امروزه از تهدید نرم استفاده می‌کنند.

۸- تهدید نرم :

جنگ‌نرم در حقیقت شامل هرگونه اقدام روانی و تبلیغات رسانه‌ای است که جامعه یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشودن آتش، رقیب را به انفعال یا شکست وا می‌دارد. جنگ روانی، با شگردها و شیوه‌های متنوعی اجرا می‌شود و باید آن را یکی از اشکال و زیر مجموعه‌های جنگ نرم دانست. جنگ رایانه‌ای و اینترنتی و راه‌اندازی شبکه‌های رادیویی و تلویزیونی و... نیز اشکال دیگر جنگ نرم هستند.

کلید خوردن جنگ نرم علیه ایران در مقطع فعلی را باید ناشی از گسترش حس تنفر از آمریکا در جهان دانست که به نظر سران کاخ سفید، ایران مرکز اصلی ایجاد این تنفر و گسترش آن است و در آمریکا برای مقابله با این موج، نیروی واکنش سریع تشکیل شده است؛ تا اولاً به خنثی‌سازی نفوذ معنوی ایران در کشورهای اسلامی و منطقه‌ی خاورمیانه بپردازد و ثانیاً با القای خطرناک بودن ایران برای امنیت همسایگان، اذهان عمومی از اقدامات و نقشه‌های ایالات متحده منحرف شود. سرمایه‌گذاری هنگفت غرب

در زمینه‌ی اطلاعات، بستر لازم برای راه‌اندازی جنگ مجازی (سایبر) علیه هر کشوری که در مغایرت با سیاست‌ها و منافع آن باشد را فراهم کرده است. جنگ نرم در پی از پای درآوردن اندیشه و تفکر جامعه‌ی هدف است تا حلقه‌های فکری و فرهنگی آن را سست کند و با بمباران خبری و تبلیغاتی، در نظام سیاسی-اجتماعی حاکم تزلزل و بی‌ثباتی تزریق کند.

پروژه‌ی ناتوی فرهنگی که چندی پیش رهبر انقلاب آن را مورد تأکید و توجه قرار دادند، مشتمل بر خط تهاجمی دشمن و تلاش معاندان نظام برای ورود از عرصه‌های فرهنگی، هنری و رسانه‌ای است تا به سیاه‌نمایی علیه ایران بپردازند. رویکرد اصلی ناتوی فرهنگی، جنگ نرم و هدف اصلی آن فروپاشی پیوندهای هم‌گرایانه ملتی است که حدود سه دهه با تمام فشارها و کاستی‌ها، صبر و مدارا پیشه کرده و راه پیشرفت و مقاومت در برابر زورگویی و انحصارطلبی دشمنان را برگزیده است.

آمریکا و جریان صهیونیسم بین‌الملل برای عملیاتی ساختن جنگ نرم و ناتوی فرهنگی علیه جمهوری اسلامی ایران، طی سال‌های گذشته راهکارهای مختلفی آزمایش کرده‌اند. سرمایه‌گذاری در رسانه‌های دیداری و شنیداری، آژانس‌های تبلیغاتی و خبری و کمپانی‌های فیلم‌سازی برای ارایه‌ی تصویری سیاه و خطرناک از جمهوری اسلامی ایران برای افکار عمومی جهان که یکی از نمونه‌های برجسته‌ی آن، ساخت و پخش فیلم ضدایرانی "۳۰۰" بوده، گوشه‌ای از این اقدامات به شمار می‌آید.

۹- سطوح قدرت نرم :

قدرت نرم از سه سطح تشکیل می‌شود:

الف) سطح راهبردی

ب) سطح میانی

ج) سطح تاکتیکی

در سطح راهبردی که اولین سطح قدرت نرم است، قدرت متوجه رهبران و نخبگان یک کشور است و بالاترین سطح رویارویی قدرت نرم با تهدید نرم را شامل می‌شود. در این سطح، هدف افزایش قدرت، هنجارسازی خود و تضعیف قدرت حریف در صحنه‌ی بین‌المللی است و هدف حریف هم از تهدید نرم در این سطح، اولاً شناسایی نخبگان و رهبران فکری جامعه و ثانیاً ارعاب و تأثیرگذاری در آن‌ها است.

با توجه به موقعیت تاریخی کهنی که ایران دارا است و موقعیت سوق‌الجیشی و جغرافیایی که ما در آن قرار داریم، همواره دشمن در کمین بهره‌گیری از موقعیت‌هاست. پس زمینه‌سازی جهت اتحاد سیاسی و اقتصادی و فرهنگی در جهان اسلام، تشنج‌زدایی و پیش‌برد صلح و امنیت در منطقه و جهان، تحرک دیپلماتیک و حضور موفق در عرصه‌های بین‌المللی، از جمله مواردی است که باعث ارتقاء قدرت نرم ما می‌شود.

در سطوح میانی این سطح از قدرت نرم منحصراً به مردم و قدرت ملی تکیه دارد و از فرهنگ عامه متأثر می‌شود. در این سطح، افکار عامه از تصمیمات نخبگان و رهبران جامعه حمایت می‌کند و به آن‌ها مشروعیت می‌بخشد. در مقابل، هدف تهدید نرم در این سطح، ایجاد شکاف میان نخبگان سیاسی و فرهنگی و آحاد عمومی جامعه است. یعنی می‌خواهند مردم را از یک جماعت همراه تبدیل به جماعتی بی‌تفاوت، معارض و مخالف کنند و برای رسیدن به این هدف از ابزارهایی مثل تشویق به نافرمانی مدنی استفاده می‌کند.در سطح تاکتیکی این سطح از رویارویی قدرت نرم در سطح نیروهای مسلح صورت می‌گیرد و هدف این سه سطح از قدرت نرم باید توأمان و همراه هم مورد توجه قرار گیرد و سعی شود در هر سه سطح قدرت‌دهی و قدرت نرم جامعه افزایش پیدا کنند تا بتواند در مقابل تهدیدات نرم مؤثر واقع شود.

۱۰-نتیجه‌گیری:

«آگاهی رکن دوم مبارزه با جنگ نرم سایبری است »

امروز که رهبر عزیز انقلاب اسلامی و فرماندهی معظم کل قوا حضرت آیت ا... خامنه ای مدظله العالی همه ما را نسبت به جنگ نرم توسط استکبار و دشمنان انقلاب و بدخواهان ملت ایران هشدار دادند، بحث عملیات روانی در حوزه جنگ‌نرم از اهم واجبات است و در واقع پاسخ جنگ‌نرم یا عملیات روانی دشمن، دفاع نرم و عملیات روانی تهاجمی و دفاعی برعلیه دشمن محسوب می‌شود.

با پیچیده‌تروکوچک‌تر شدن جهان به واسطه رشد فزاینده وسایل ارتباط جمعی از قبیل اینترنت و شبکه‌های‌ماهواره‌ای، معادلات گذشته در تنظیم روابط بین کشورها تا حدود زیادی به‌هم خورده و جای خود را به معادلات جدیدی داده است؛ به‌گونه‌ای که به-جای به‌کارگیری مستقیم زور، توجه قدرت‌ها به استفاده از قدرت-

نرم و ایجاد تغییرات ازطریق مسالمت‌آمیز با به‌کارگیری شیوه‌های نوین مداخله در امور داخلی کشورها جلب شده است. جنگ‌نرم در برابر جنگ سخت در حقیقت شامل هرگونه اقدام روانی و تبلیغات رسانه‌ای که جامعه هدف یا گروه هدف را نشانه می‌گیرد و بدون درگیری نظامی و گشوده شدن آتش، رقیب را به انفعال یا شکست وامی‌دارد انگاشته می‌شود.

با امعان‌نظر به نقاط ضعف اصلی در دفاع سایبر :

- بررسی هویت و مکان مهاجم.
- شناسائی نیت مهاجم.
- تشخیص حمله‌های از قبل طراحی شده.
- بررسی و ارزیابی تلفات بعد از جنگ.

فضای سایبر، فضایی است مجازی که به‌واسطه ابزاری غیرفیزیکی، کارکردی دوگانه دارد.هم باعث ارتقا سطح فکری و هم باعث تشویش اذهان عمومی و شست و شوی مغزی می‌شود.لازم است برای شناخت فرصت‌ها و تهدیدها در عرصه جنگ‌نرم و در حوزه سایبر ،ابزارهای موجود را بشناسیم و بدانیم کدامیک امکان ارتباطی وسیع‌تری را فراهم می‌کنند و قدرت نفوذ بیشتری دارد.درنظر داشته باشیم که دانشمندان علوم ارتباطات ۳ موج اصلی را در انقلاب ارتباطات و رسانه از هم تمییز می‌دهند:

موج اول رسانه‌های چاپی(printed media) مانند کتاب، مطبوعات و نشریات.

موج دوم رسانه‌های تصویری و صوتی(Visual media) مانند تلویزیون یا ویدئو .

موج سوم رسانه‌های دیجیتال (Digital media) مانند چند رسانه-ای ها و یا اینترنت.

لذا برمبنای رویکرد آگاه سازی، پاک‌سازی و حضور در شبکه‌های اجتماعی و بعضا مقابله به مثل، راهبردهای ذیل به‌عنوان راه‌کار جهت مقابله با جنگ‌نرم سایبری در این مقطع پیشنهاد می‌شود :

- راه‌اندازی سایت‌های اینترنتی و ارایه‌ی نرم‌افزارهای جاسوسی به‌عوامل وابسته در داخل کشور، تا ابعاد مختلف جنگ رسانه‌ای به‌شکل اثربخش‌تر طراحی و اجرا شود.

- تلاش جهت ایجاد تقابل سیاسی بین سران ارشد نظام اسلامی و القای این‌که "جنگ قدرت" در جمهوری اسلامی بین چند طیف در جریان است و نهایتاً فلان طیف یا فلان گروه از پیش، پیروز شده و یا شکست خورده‌اند. می‌توان گفت پازل رسانه‌ای آمریکا برای تحت فشار قراردادن ایران اسلامی طراحی شده و راهکار خنثی‌سازی و بی‌اثر کردن تلاش‌های دشمنان، ایجاد فضای هم‌نوایی و هم‌گرایی بین نیروهای درون نظام و عمل به مقتضیات اتحاد ملی به‌عنوان رهیافت راهبردی نظام اسلامی است. افشای حقایق و اوضاع داخلی آمریکا و نیز برملا نمودن توطئه‌های غرب در خاورمیانه و جهان اسلام و نیز تقویت زمینه‌های "انسجام ملی" در زمره‌ی راهکارهایی هستند که می‌توانند در ناکامی نقشه‌های مراکز راهبردسازی دولت آمریکا در ایجاد جنگ نرم علیه ایران تأثیرگذار باشند.

منابع‌وماخذ :

۱. تسبیحی، اکبر، " انقلاب اطلاعات و اثرات آن بر امور نظامی "، فصلنامه ره آورد مدیریت نظامی، شماره ۱و ۲۸ -۱۳۷۹.

۲. جعفری، رضا، " قرن بیست و یکم و جنگهای کامپیوتری " ، روزنامه کیهان، ۱۳۷۶.

۳. سلامی، حسین، "جنگ های آینده" ، دانشگاه عالی دفاع ملی ، تهران ، ۱۳۸۳.

۴. صادقی، میر محمد،"جنگ شبکه محور پاسخی نظامی به چالش ها ونیازهای آینده"(مقاله علمی)، دانشگاه صنعتی مالک اشتر، تهران، ۱۳۸۳.

۵. فهیمی، مهدی،"عصراطلاعات و میزان تاثیر علم و فن آوری درجنگ های اخیر"(مقاله علمی)، دانشگاه مالک اشتر، ۱۳۸۳.

۶. والتز، ادوارد، جنگ اطلاعات-اصول عملیات ، ترجمه مهندس اکبر رنجبر ، دکتر حسن حاج قاسم و مهندس محمود فخرائی ، انتشارات موسسه آموزشی و تحقیقاتی صنایع دفاع- فاوا، تهران ، ۱۳۸۵.