مجله جهانی رسانه- نسخه فارسی

دوره ۶، شماره ۲، شماره پیاپی ۱۲، صفحات ۱۵۱- ۱۶۶

منتشر شده در پاییز ۱۳۹۰

مقاله دانشجویی

گونه‌شناسی نبردهای اطلاعاتی و جنگ‌های سایبری

فرشید دانش

دانشجوی دکتری، علوم کتابداری و اطلاع‌رسانی، دانشگاه فردوسی مشهد

farshiddanesh@gmail.com

راضیه زاهدی

دانشجوی کارشناسی ارشد، کتابداری و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی تهران

zahedirazieh@gmail.com

مجله جهانی رسانه- نسخه فارسی

مجله علمی- پژوهشی الکترونیک در حوزه ارتباطات و رسانه
منتشر شده توسط دانشکده علوم اجتماعی، دانشگاه تهران، ایران

www.gmj.ut.ac.ir

چکیده

هدف از تدوین این مقاله، پرداختن به مفاهیم اساسی موجود برای درک مفهوم نبرد اطلاعاتی است. استفاده از اطلاعات در نبردها امری جدید نیست و به گذشته‌های دور باز می‌گردد. با این وجود نبرد اطلاعاتی اصطلاح جدیدی است که پدیده‌ی موج سوم و محصول فرعی انقلاب رایانه‌ای است. در این مقاله پس از ارائه مقدمه‌ای در مورد نبرد اطلاعاتی، تاریخچه نبرد در جهان و مفهوم و تعاریف نبرد اطلاعاتی تبیین و پس از آن به سطوح و راهکارهای مورد استفاده در نبرد اطلاعاتی اشاره می گردد. در انتها، پس از معرفی انواع ابزارهای مورد استفاده در این نوع نبرد، راهبردهای مقابله با آن ذکر می‌شود. نبرد اطلاعاتی محدود به کاربردهای سیاسی، نظامی و امنیتی نیست و در سطوح فردی و گروهی نیز شاهد وقوع آن هستیم؛ بنابراین آگاهی نسبت به این نوع از نبرد در سطح فردی، سازمانی و ملی می‌تواند امکان پیشگیری و مقابله با آن را فراهم آورد.

کلیدواژه‌ها: نبرد اطلاعاتی، امنیت اطلاعات، اطلاعات، جنگ سایبری

مقدمه

اطلاعات از دیدگاه‌های گوناگون و گاه بسیار متفاوت مورد مطالعه قرار گرفته و رویکردهای متفاوت به این مفهوم همواره محل بحث و تبادل نظر بوده است. توجه به ارزش اطلاعات به عنوان کالایی راهبردی و نقش آن در تصمیم‌گیری‌ها و برنامه‌ریزی‌ها، یکی از این رویکردها است که در اقتصاد اطلاعات نیز به عاریت گرفته شده است. همچنین در همه شیوه‌های توسعه دانش و اطلاعات از عناصر مهم است، چون فرآیند تولید همواره بر سطحی از دانش و پردازش اطلاعات استوار است. با این حال ویژگی شیوه توسعه متکی به اطلاعات، کار دانش بر روی دانش به عنوان منبع اصلی بهره‌وری است (کاستلز، ۱۳۸۰، ص. ۴۵).

علاوه بر این، عصر رایانه با توانایی خاص خود در تبادل اطلاعات، ارزشی چند برابر به اطلاعات داده و آن را وارد عرصه‌های مختلف زندگی انسان کرده است. یکی از این عرصه‌ها، نبرد و جنگ میان افراد، سازمان‌ها و ملل گوناگون است. اطلاعات همواره به عنوان عاملی اساسی در جنگ‌ها مطرح بوده است. کلوسویتز[۱] می گوید: "دانش ناکافی از موقعیت می‌تواند موجب از حرکت ایستادن عملیات نظامی شود" (به نقل از ک لندون، ۱۹۹۴، ص. ۲). سانتزو[۲] نیز اطلاعات را عاملی اساسی در جنگ می‌داند (به نقل از مک لندون، ۱۹۹۴، ص. ۵). این بیانات، اهمیت اطلاعات را به عنوان سرمایه راهبردی ملت‌ها و دولت‌ها بیش از پیش آشکار می‌سازد. اهمیت اطلاعات راهبردی به اندازه‌ای است که می‌تواند موجب پیروزی یا شکست نیروهای نظامی و سیاسی در سراسر جهان گردد (دوروتی، ۱۹۹۹).

تافلر معتقد است سه موج نبرد در تاریخ بشر وجود دارد، این سه موج عبارتند از: موج کشاورزی، صنعتی و اطلاعاتی. موج نبردهای کشاورزی با انقلاب کشاورزی و شکل‌گیری جوامع در جهان آغاز شد. موج دوم، موج نبردهای صنعتی بود. نمونه بارز این نوع نبرد، جنگ جهانی دوم بود که پانزده میلیون تلفات به همراه داشت. دکترین اصلی نبرد در این دوره، نابودی همه چیز برای پیروزی در جنگ بود. موج سوم، موج نبردهای اطلاعاتی است (تافلر، ۱۹۹۳). در نبردهای اطلاعاتی، دکترین‌های نظامی تغییر کرده و می‌تواند فعالیت‌های جمع‌آوری اطلاعات مربوط به جنگ، کسب اطمینان از صحت اطلاعات، پخش اطلاعات نادرست

برای تضعیف روحیه دشمن یا مردم عادی و تحلیل و کم کردن کیفیت اطلاعات طرف مقابل را در بر گیرد (جهانگیری، ۲۰۰۸ ، ص. ۴). جدول شماره (۱)، به طور خلاصه ویژگی‌های سطوح سه‌گانه نبردها را نشان می‌دهد.

جدول۱. ویژگی‌های موج‌های سه گانه نبردها (هاینی[۳]، ۱۹۹۷، ص. ۹)

موج‌ها	اول	دوم	سوم
توصیفگر	کشاورزی	صنعتی	اطلاعاتی
تأمین‌کنندگان امنیت	سربازان غیرحرفه‌ای و مزدوران	شهروندان	رهبران دانش مدار
نمادهای اجتماع و سیاست	قبیله، شهر، ایالت و خانواده	کارخانه‌ها و صنایع	شرکت‌های چند ملیتی و جهانی
نماد اقتصاد	تجارت	پول	داده‌ها در پایگاه‌های اطلاعاتی
نبردها	نبردهای قبیله‌ای و قومی	ارتش‌های منظم	نبردهای اطلاعاتی
انواع سلاح‌ها	سلاح‌های ساخته شده از باروت	سلاح‌های شیمیایی و اتمی	نرم‌افزارهای نابودکننده داده‌ها
رهبری	ساختار رهبری و قدرت سلسله مراتبی	ساختار رهبری و قدرت از بالا به پایین	ساختار قدرت و رهبری مسطح
استفاده از اطلاعات در نبرد	بله	بله	بله
استفاده از فنآوری اطلاعات در نبرد	خیر	بله	بله
نبرد اطلاعاتی	خیر	خیر	بله

همانطور که جدول بالا نشان می‌دهد، استفاده از اطلاعات در هر سه موج نبرد قابل مشاهده است. با این وجود مفهوم نبرد اطلاعاتی خاص موج سوم است. داده‌ها در پایگاه‌های اطلاعاتی، نماد اقتصادی نبرد اطلاعاتی است و نرم‌افزارها به عنوان سلاح مورد استفاده در این موج، مطرح هستند.

نبرد اطلاعاتی، مفهوم جدیدی نیست، بلکه پدیده موج سوم و محصول فرعی انقلاب رایانه‌ای است. این واژه به تکنیک‌های متفاوت برای کنترل یا تحت تأثیر قرار دادن دانش، قضاوت و تصمیم‌گیری طرف مقابل

باز می‌گردد (اسمیت[۴]، ۲۰۰۰ ، ص. ۱). جنگ اطلاعات، جنگی به تمام معناست. اطلاعات و توانایی به کارگیری آن، نیروی جدیدی را به نبرد تزریق می‌کنند. با مجهز کردن نیروها به اطلاعات، محدوده تحت نفوذ، سرعت نبرد و دقت آن افزایش می‌یابد (مالونون[۵]، ۱۹۹۸ ، ص. ۱۸۰). با توجه به مفهوم اطلاعات و نبرد اطلاعاتی، دو نوع ارزش برای منابع اطلاعاتی در نبردهای اطلاعاتی قابل تصور است. این دو نوع ارزش عبارتند از: ارزش بازاری و ارزش عملیاتی. ارزش بازاری، دارای مقدار کمّی است و این کمیت از هزینه‌ای که در بازار برای این اطلاعات پرداخت می‌شود، بدست می‌آید. ارزش عملیاتی نیز ناشی از منافعی است که با استفاده از این منبع بدست می آید، گرچه ممکن است قابل اندازه گیری کمّی باشد، ولی همیشه هم اینطور نیست؛ مثلاً اطلاعات مربوط به محل استقرار نیروهای دشمن و یا معالجهٔ سرطان که منجر به نجات جان میلیون‌ها انسان می‌شود، قابل اندازه‌گیری کمّی نیست (سلماسی‌زاده، ۱۳۸۰).

نبرد اطلاعاتی هر نوع رسانه را می‌تواند هدف قرار داده و یا از آن سوء استفاده کند. رسانه می‌تواند نوشتاری، محیط ذخیره مغناطیسی، محیط انتشاری، مخابرات راه دور، رایانه و سیستم‌های اطلاعاتی باشد. عملیات اصلی در نبرد اطلاعاتی هدف قرار دادن منابع اطلاعاتی طرف مقابل بوده و شامل عملیات آفندی و پدافندی است و البته این عملیات به خاطر ارزشی که منابع اطلاعاتی برای اشخاص و کشورها دارد، انجام می‌شود. هدف عملیات آفندی افزایش منابع اطلاعاتی برای حمله‌کننده و کاهش آن برای مدافعان است و عملیات پدافندی نیز برای مقابله با کاهش ارزش منابع اطلاعات انجام می‌گیرد (سلماسی‌زاده، ۱۳۸۰). اکنون یکی از چالش‌های پیش روی کشورها، رویارویی با این پدیده نو ظهور است و اغلب مراکز مطالعات نظامی و راهبردی دنیا، نبرد اطلاعاتی را در زمره دکترین‌های نظامی خود قرار داده‌اند.

نبرد اطلاعاتی و جنگ سایبری دو بیان متفاوت از یک مفهوم هستند که در متون فارسی کمتر به آن پرداخته شده است. برای درک این مفهوم لازم است ابتدا تعاریف متعدد آن مرور شوند، سپس باید راهکارهای مورد استفاده در آن را مورد مطالعه قرار داد تا مشخص گردد چه مواردی در زمره نبرد اطلاعاتی و جنگ سایبری قرار می‌گیرد. در مرحله بعد باید مشخص گردد این نوع نبرد در چه سطوحی رخ می‌دهد؟

آیا تنها در سطح ملی مطرح شده یا می‌تواند افراد و سازمان‌ها را هم شامل شود؟ در نهایت ابزارهای مورد استفاده در نبرد اطلاعاتی چیست و چه راهبردهایی برای مقابله با آن می‌توان اتخاذ کرد؟ در این مقاله می کوشیم با پاسخگویی به این پرسش‌ها، ضمن آگاهی از مفهوم و گونه‌شناسی نبرد اطلاعاتی و جنگ سایبری، مؤلفه‌ها و عناصر آن را تبیین و تحلیل کرده تا زمینه‌ی شناخت، کنترل و مقابله‌ی با آن را فراهم آوریم.

روش و مراحل پژوهش

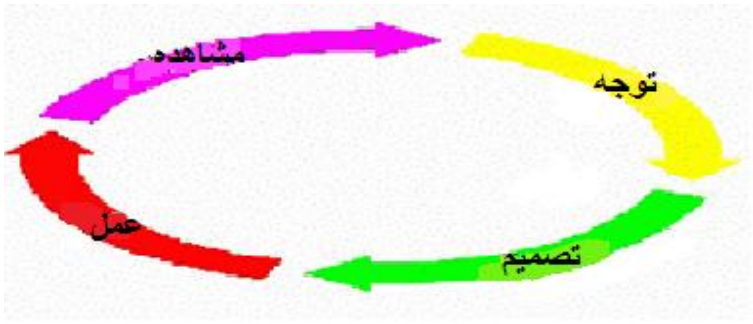
در این مقاله برای پاسخگویی به پرسش‌های پژوهش، به مرور مطالعات این حوزه می‌پردازیم. در همین راستا، مفهوم نبرد اطلاعاتی، راهکار، سطوح و ابزارهای مورد استفاده در آن توضیح و تبیین می‌شوند. سپس با تحلیل یک نبرد اطلاعاتی، مراحل و مولفه‌های آن را مشخص می‌کنیم. در نهایت با جمع بندی یافته‌ها، پیشنهادها و راهکارها برای کنترل و مقابله با نبرد اطلاعاتی ارائه می‌شود.

تبیین مفهوم نبرد اطلاعاتی و جنگ سایبری

یکی از چالش‌های پیش رو در رابطه با تبیین مفهوم نبرد اطلاعاتی، فقدان تعریفی رسمی از این مفهوم است. مهمترین دلیل این امر، از یک سو نو بودن این گونه از نبرد و از سوی دیگر تنوع مفهومی و معنایی نبرد اطلاعاتی است؛ چنانچه برخی از دانشمندان جنبه نظامی و بعضی دیگر جنبه اینترنتی آن را مورد ملاحظه قرار می‌دهند (هاینی، ۱۹۹۷ ، ص. ۴). در هر حال، امروزه اصطلاح نبرد اطلاعاتی بیشتر به معنی جنگ سایبری به کار می‌رود (بلمی[۶]، ۱۹۹۸). ویلسون[۷] (۲۰۰۴) نیز نبرد اطلاعاتی و جنگ سایبری را دو بیان متفاوت از یک مفهوم دانسته که در آن با استفاده از فنآوری، جریان اطلاعات مختل شده تا از این طریق توانایی یا تمایل مبارزه در طرف مقابل تحت تأثیر قرار گیرد. کریلی[۸] (۲۰۰۱) اذعان می‌دارد که نبرد اطلاعاتی به شیوه‌های گوناگونی تعریف شده است. اما اجماع نظر صاحب‌نظران بر آن است که نبرد اطلاعاتی زمانی روی می‌دهد که دشمنان با بهره‌برداری از ابزارها و تکنیک‌ها، انقلاب اطلاعاتی راه بیاندازند. دنینگ[۹] (۲۰۰۰) نیز بر این باور است که هر جا نبرد اطلاعاتی روی دهد، عنصری از ترس در جایی از معادله دیده می‌شود. به عبارت دیگر افراد، سازمان‌ها و سازمان‌های جاسوسی کشورها به خاطر ترس از به خطر افتادن منافع‌شان دست به نبرد اطلاعاتی می‌زنند. شوراتو[۱۰] (۱۹۹۴) هم در تعریف خویش، نبرد اطلاعاتی را شامل

اقداماتی می‌داند که از طریق آن، یک طرف بر دیگری برتری اطلاعاتی حاصل می‌کند و این برتری از طریق تحت تأثیر قرار دادن اطلاعات دشمن، فرایندهای مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای به دست می‌آید. تبلیغات گسترده و شیوع ترس بین مردم، حمله به زیرساخت‌ها (مانند ذخایر انرژی، حمل و نقل، ارتباطات و ...) و استفاده از رسانه‌ها می‌توانند از نشانه‌های نبرد اطلاعاتی باشد (هرد[11]، ۲۰۰۳ ؛ سندرل[12]، ۲۰۰۴ ، ص. ۵). با در نظر گرفتن این تعاریف می‌توان گفت در نبرد اطلاعاتی، اطلاعات تغییر داده شده یا در جریان آن خللی ایجاد می‌شود. در این نبرد سعی بر آن است با ابزارهای گوناگون، سطح آگاهی طرف مقابل کاهش یافته و در نتیجه امکان کنترل شرایط از جانب آنان از بین برود.

یکی از مفاهیمی که اغلب برای به تصویر کشیدن مفهوم نبرد اطلاعاتی مورد استفاده قرار می‌گیرد مدل او.او.دی.ای[13] است. این مدل از چهار مرحله مشاهده، توجه، تصمیم و عمل تشکیل شده است. تصویر شماره (۱)، این مدل را نشان می‌دهد:



تصویر شماره (۱). حلقه مشاهده، توجه، تصمیم و عمل(کروفورد[14]، ۱۹۹۴)

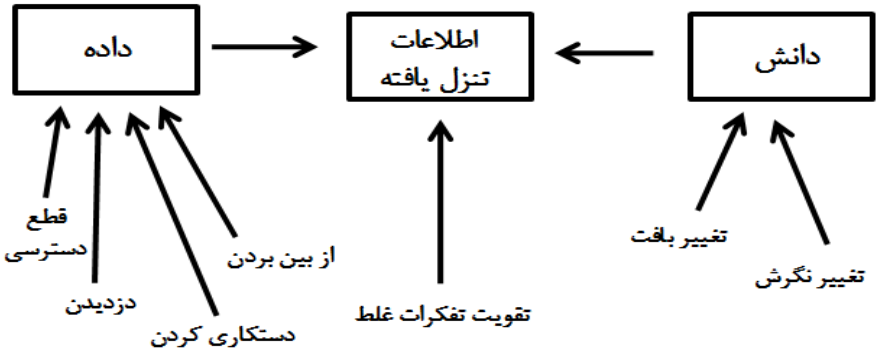
در این حلقه، ابتدا حمله‌کننده شرایط میدان نبرد را مشاهده می‌کند؛ سپس حمله‌ی خود را بر اساس فرصت‌ها و تهدیدهای مشاهده شده در مرحله قبلی، متمرکز می‌کند؛ زمانی که هدف تعیین و تمرکز روی آن حاصل شد، حمله کننده تصمیم می‌گیرد که کدام بخش از عملیات را به اجرا درآورد. با توجه به اطلاعات قبلی در این مرحله حمله آغاز می‌شود. نکته مهم در این مدل، فرایندی بودن آن است؛ چرا که زمانی که

یک طرف حمله را آغاز می‌کند، طرف دوم مرحله مشاهده را از سر می‌گیرد و شرایط را برای انتخاب عکس العمل مناسب مشاهده می‌نماید. مدت زمان لازم برای کامل شدن چرخه، به اندازه حلقه بستگی دارد؛ اندازه حلقه نیز تحت تأثیر عواملی نظیر زمان لازم جهت گردآوری، تحلیل و اشاعه‌ی مشاهدات و همچنین زمان لازم جهت تمرکز روی حمله و تصمیم‌گیری برای حمله است (کروفورد، ۱۹۹۴).

تعاریف و مفاهیم متعدد که در بالا به آن اشاره شد، حاکی از گستردگی موضوعی این مفهوم و چند مرحله‌ای بودن آن دارد. همین امر سبب شده است که راهکارهایی که در نبرد اطلاعاتی به کار گرفته می شوند نیز متعدد باشند. در ادامه، به این راهکارها اشاره می‌شود.

راهکارهای مورد استفاده در نبرد اطلاعاتی

با توجه به مفاهیم داده، اطلاعات و دانش؛ می‌توان چندین تاکتیک برای نبرد اطلاعاتی برشمرد. تصویر شماره ۲ راهبردهای مورد استفاده در نبرد اطلاعاتی را با توجه به مفاهیم داده، اطلاعات و دانش ترسیم می کند:



تصویر۲. راهکارهای مورد استفاده در نبرد اطلاعاتی(هاچینسون[15]،۲۰۰۲، ص. ۴۱۱)

با توجه به شکل، این مطلب قابل برداشت است که اگر هدف حمله، داده است، راهکارهای زیر قابل اجرا است: کاهش یا قطع دسترسی به داده: این راهکار با حمله به سخت‌افزار و یا نظام‌های حاوی داده و یا مجموعه‌ای از داده‌ها انجام می‌شود. با توجه به میزان ارزش و اهمیت داده‌ها، این راهکار می‌تواند از تأخیر دسترسی به داده تا غیرقابل استفاده کردن آن را شامل شود.

از بین بردن داده: تخریب داده به صورت تخریب فیزیکی محمل ذخیره داده و یا خود داده امکان‌پذیر است. در این صورت، داده در زمانی که مورد نیاز است، غیرقابل استفاده می گردد. البته عده‌ای معتقدند که تنها تخریب محمل ذخیره امکان‌پذیر است و نه خود داده.

سرقت داده: بسیاری از داده‌ها محرمانه بوده و دارای ارزش رقابتی هستند. کسی که قصد دزدیدن این اطلاعات را دارد می‌تواند از طریق مذاکره و دادن منافعی به دیگری این کار را انجام دهد.

دستکاری داده: در این راهکار، داده‌ها حذف، اضافه و یا اصلاح و تجدید نظر می‌شوند. افرادی که قصد کلاه‌برداری دارند معمولاً از این شیوه استفاده می‌کنند.

از سوی دیگر، راهکارهای که با دانش مرتبط هستند، دوگونه‌اند: تغییر بافت و زمینه‌ای که داده در آن تفسیر می‌شود و تغییر نگرش مردم نسبت به آن داده. این دو راهکار بسیار به یکدیگر نزدیک هستند. با این تفاوت که در راهکار اول، تمرکز بر تغییر شرایط است؛ مانند تغییر محل و یا تغییر اوضاع سیاسی، اما راهکار دوم بر روی مردم و نحوه تفکر آنها تمرکز دارد و مواردی چون تبلیغ و فتنه‌انگیزی را در بر می‌گیرد.

تمامی راهکارهای اعمال شده بر روی داده و یا دانش، منجر به تقویت تصورات غلط شده و تنزل اطلاعات را در پی دارد (هاچینسون،۲۰۰۲ ، ص.۴۱۲). به عبارتی، راهکارهای مورد استفاده در نبرد اطلاعاتی اطلاعات غلط را در اختیار افراد قرار می‌دهد؛ به‌گونه‌ای که این اطلاعات از جانب آنها مورد پذیرش واقع می‌شود. این شرایط باعث ایجاد تفکر غلط نسبت به حادثه یا شیء شده و شرایط را به نفع دشمن رغم می‌زند. نکته‌ی دیگری که در کنار مفهوم و راهکارهای مورد استفاده در نبرد اطلاعاتی حائز اهمیت است، توجه به سطوحی است که در نبرد اطلاعاتی مورد حمله قرار می‌گیرند. بر خلاف تصور عموم، نبرد اطلاعاتی به نبرد میان کشورها محدود نمی‌شود؛ بلکه این نوع نبرد می‌تواند در سطح فردی و جهانی نیز مطرح باشد. در ادامه این موضوع شرح داده می‌شود.

سطوح نبردهای اطلاعاتی

شوارتو(۱۹۹۴) برای تعریف نبرد اطلاعاتی، راهی متفاوت برگزیده است. وی نبرد اطلاعاتی را به سه سطح دسته‌بندی کرده است: نبرد اطلاعاتی فردی، گروهی و جهانی. در سطح فردی، حمله به منابع اطلاعاتی اشخاص، پایگاه‌های اطلاعاتی و هر محلی که اطلاعات فردی در آنجا ذخیره شده است، صورت می گیرد. امروزه با توجه به گستردگی خدمات الکترونیکی توسط دولت‌ها و مؤسسات، بخش اعظمی از اطلاعات خصوصی افراد در اختیار سازمان‌های خدمت‌رسان قرار دارد. از جمله این اطلاعات می‌توان به صورتحساب های مالی، شماره حساب‌ها، پرونده‌های پزشکی و خدمات مربوط به سلامت و اطلاعات حقوقی افراد اشاره نمود. گاهی اوقات مهاجمان با نیات گوناگون مراکز ذخیره اینگونه اطلاعات را مورد حمله قرار می‌دهند و تمامی اطلاعات شخصی افراد را فاش می‌سازند (شوارتو، ۱۹۹۴). در این سطح از نبردهای اطلاعاتی؛ امکان نابودی هویت فردی، شغلی و حقوقی افراد وجود دارد. نبردهای اطلاعاتی فردی می‌تواند با سطوح دوم و سوم نبردها یعنی نبردهای گروهی و جهانی نیز پیوند برقرار نماید.

سابقه نبرد اطلاعاتی در سطح دوم به دوران جنگ سرد باز می‌گردد، زمانی که نیروهای نظامی و اطلاعاتی روسیه و ایالات متحده امریکا به دنبال جمع‌آوری اطلاعات نظامی از یکدیگر بودند. در نبردهای اطلاعاتی گروهی، کمپانی‌ها و شرکت‌های بزرگ با یکدیگر به نبرد می‌پردازند. امروزه نبرد اطلاعاتی در این سطح ابعاد تازه‌ای به خود گرفته است.

در سطح سوم، نبرد اطلاعاتی در سطح جهانی مطرح می‌شود. در این نوع نبرد اطلاعاتی، صنایع و اقتصاد جهانی مورد حمله قرار می‌گیرد و محرمانه‌ترین اطلاعات رقبا به سرقت رفته و علیه آنها استفاده می‌شود. نکته مهم در این سطح خرابی‌ها و چالش‌های غیرقابل تصور ناشی از این نوع حمله‌ها می‌باشد. در این سطح دیگر افراد و منافع اقتصادی عامل حیاتی نیستند؛ حمله‌ها از هزاران کیلومتر دورتر انجام می‌شود و نتایج و تأثیرات آن غیرقابل تصور است. برای مثال با استفاده از سلاح‌های نسل سوم، تروریست‌ها می‌توانند به راحتی نظام‌های اقتصادی، علمی و اجتماعی دشمنان خود را مورد حمله قرار داده و آنها را از بین ببرند (شوارتو، ۱۹۹۴).

ابزارهای مورد استفاده در نبردهای اطلاعاتی

هر نبردی سلاح‌های خاص خود را می‌طلبد، در نبردهای اطلاعاتی نیز که نسل سوم نبردها محسوب می‌شود؛ از ویروس‌های رایانه‌ای، کرم‌ها، اسب‌های تروا، بمب‌های منطقی، تله‌های نرم‌افزاری، ماشین‌های نانو و میکروب‌های رایانه‌ای، پارازیت، فرکانس‌های رادیویی با انرژی بالا و پالس‌های الکترومغناطیسی به عنوان ابزار نبرد استفاده می‌شود.

دبورا و گنجمی[۱۶] (۱۹۹۴) بر این باورند که ویروس‌های رایانه‌ای شایع‌ترین ابزار مورد استفاده در نبردهای اطلاعاتی هستند. ویروس برنامه‌ای رایانه‌ای است که به سرعت تکثیر، و زمانی فعال می‌شود که رایانه میزبان آن برنامه را اجرا کند. پس از اولین اجرا، ویروس تمام برنامه‌های رایانه میزبان را آلوده و به اطلاعات آنها دسترسی پیدا می‌کند. قدرت نفوذ ویروس‌ها در شبکه‌های اطلاعاتی بسیار بالا است، برای نمونه، با توجه به دیجیتالی شدن شبکه‌های مخابراتی کشورها، ویروس‌ها می‌توانند به شبکه‌های مخابراتی نفوذ کرده و خطوط تلفن را با اختلال و یا قطعی مواجه نمایند.

ابزار دیگری که در نبردهای اطلاعاتی مورد استفاده قرار می‌گیرد، کرم‌ها هستند. کرم‌ها برنامه‌های رایانه‌ای مستقلی هستند که در یک شبکه اطلاعاتی وارد شده و از یک رایانه به رایانه دیگر رخنه کرده و تمامی اطلاعات آنها را به سرقت می برند. کرم ها داده‌ها را از بین نمی‌برند، بلکه در شبکه اطلاعاتی گسترده شده و ارتباطات را دچار اختلال می کنند. همچنین کرم‌ها به راحتی می‌توانند اطلاعات را پاک کرده و یا دستکاری نمایند. یکی از بارزترین نمونه‌های نفوذ کرم‌ها در شبکه‌های اطلاعاتی مالی است. مهاجمان از این ابزار جهت نفوذ در برنامه‌های بانکداری الکترونیکی استفاده می‌کنند و با دستکاری در حساب‌های دولتی و شخصی در نظام مالی کشور اختلال ایجاد می‌نمایند (دبروا و گنجمی، ۱۹۹۴).

اسب‌های تروا از دیگر ابزارهای مورد استفاده در نبردهای اطلاعاتی هستند. این برنامه‌ی رایانه‌ای، به صورت مبدل و با کارکردی فریب‌دهنده وارد شبکه‌های رایانه‌ای طرف مقابل می‌شود. مهمترین نقش این ابزار، وارد نمودن ویروس‌ها و کرم‌ها به شکل مستتر به شبکه‌های اطلاعاتی است. اسب‌های تروا در قالب برنامه‌های امنیتی وارد شبکه‌های اطلاعاتی می‌شوند. برای مثال ابزار مدیریت تحلیل شبکه‌ها، ابزاری جهت

کنترل و مسدود کردن رخنه‌های احتمالی سیستم یونیکس می‌باشد. این ابزار به صورت رایگان در محیط وب قابل دسترسی است؛ ممکن است اسب‌های تروا به صورت مستتر به این ابزار نفوذ کرده و برای استفاده‌کنندگان ایمیل‌هایی ارسال نموده و اطلاعات شخصی آنها را به سرقت ببرد. چون کاربر زمانی که از این ابزار استفاده می‌کند هیچ نشانه‌ای از اسب‌های تروا را نمی‌بیند، از این رو، اطلاعات شخصی خود را به راحتی در اختیار برنامه قرار می دهد.

بمب‌های منطقی نوعی از اسب‌های تروا هستند که برای آزادسازی ویروس‌ها، کرم‌ها و سایرنظام‌های حمله‌کننده مورد استفاده قرار گرفته و به صورت یک برنامه مستقل در سطح نظام پخش می‌شوند.

تله‌های نرم‌افزاری که به نرم‌افزارهای جاسوسی نیز معروفند، از معروفترین ابزارهای مورد استفاده در نبردهای اطلاعاتی هستند که توسط طراحان، درون سیستم‌ها قرار می‌گیرند و این امکان را فراهم می‌سازند که بتوان در هر زمانی به سیستم مورد نظر رخنه کرده و از سیستم‌های محافظتی آن عبور نمود.

استفاده از ماشین‌های نانو و میکروب‌ها خسارات جبران‌ناپذیری را به سیستم‌های اطلاعاتی وارد می‌کند. این ابزار، برخلاف ویروس‌ها، علاوه بر نرم افزار، سخت‌افزار سیستم را نیز مورد حمله قرار می‌دهد. ماشین‌های نانو روبات‌های کوچکی هستند که می‌توانند در مراکز اطلاعاتی دشمن رخنه کرده و صدمات جبران‌ناپذیری را به آنها وارد نمایند. میکروب‌ها هم می‌توانند تمامی مدارهای یکپارچه، آزمایشگاه‌های رایانه، سایت‌ها، ساختمان‌ها و حتی شهرها را نیز نابود کنند.

پارازیت در گذشته و حتی امروزه به عنوان یکی از مهمترین ابزارهای مورد استفاده در نبردهای اطلاعاتی جهت اختلال و مسدود کردن کانال‌های ارتباطی استفاده می‌شود. زمانی استفاده از این ابزار در نبردهای اطلاعاتی، هیچ گونه اطلاعاتی به گیرنده‌های دشمن نمی‌رسد. علاوه بر این، امروزه از این ابزار برای ارسال اطلاعات اشتباه به سیستم‌های اطلاعاتی طرف مقابل نیز استفاده می‌شود.

فرکانس‌های رادیویی با انرژی بالا، که از ابزارهای مورد استفاده در نبردهای اطلاعاتی هستند، قادرند سیگنال‌های رادیویی با قدرت بالا را از کار بیاندازند و خسارات سنگینی وارد نمایند؛ برای مثال می‌توانند سیستم‌ها را موقتاً خاموش نموده یا سیستم‌های سخت‌افزاری را نابود نمایند. این ابزار در واقع یک فرستنده

رادیویی است که سیگنال‌هایی را به سمت اهداف خود ارسال می‌کند. این اهداف ممکن است سرورهای شبکه‌های تجاری یا نظامی و یا حتی هواپیماها یا خودروهای در حال حرکتی باشند که مجهز به ابزارها و مدارهای الکترونیکی هستند.

پالس‌های الکترومغناطیسی از انواع دیگر ابزارهای به کار رفته در نبردهای اطلاعاتی است. تیم‌های حمله‌کننده با استفاده از این پالس‌ها؛ تجهیزات الکترونیکی، کامپیوترها و سیستم‌های ارتباطی پیرامون خود را از بین می‌برند. تفاوت این پالس‌ها با فرکانس‌های رادیویی با انرژی بالا، از یکسو کوچک بودن آنها و کم بودن میزان خرابی ناشی از آنها است؛ و از سوی دیگر، این پالس‌ها تمامی تجهیزات تحت شعاع خود را نابود می‌کنند (دبروا و گنجمی، ۱۹۹۴).

با در نظر گرفتن ابزارهای معرفی شده در این قسمت، می‌توان گفت همانند سطوح و راهکارهای مورد استفاده در نبرد اطلاعاتی، ابزارهای مورد استفاده در آن نیز متنوع و گوناگون بوده و می‌توانند آسیب‌های سخت‌افزاری و نرم‌افزاری متفاوتی به اطلاعات و تجهیزات اطلاعاتی وارد کنند. حال آنکه آگاهی از ابزارها و طریقه‌ی عملکرد آنها، مقابله با آنها را تسهیل می‌کند.

بحث و نتیجه‌گیری

منابع اطلاعاتی در همه تصمیم‌گیری‌های حساس و راهبردی نقشی کلیدی ایفاء می‌کنند. گسترش فنآوری‌های اطلاعاتی و ارتباطی نیز استفاده از منابع اطلاعاتی را گسترش داده، به گونه‌ای که شاهد استفاده از منابع اطلاعاتی در تمامی سطوح جامعه هستیم. نبرد اطلاعاتی یکی از بسترهایی است که اطلاعات در آن نقش اساسی بازی می‌کند. نبرد اطلاعاتی واژه‌ای جدید، اما مفهومی با قدمت طولانی است. این نوع نبرد در کاربرد فعلی خویش محصول انقلاب رایانه‌ای است و در سطوح فردی، گروهی و جهانی قابل مشاهده است. همچنین با افزایش وابستگی به منابع اطلاعاتی، احتمال افزایش آسیب ناشی از حملات سایبری وجود دارد. با در نظر گرفتن آسیب‌های ناشی از این گونه نبرد، لزوم آشنایی با مفهوم نبرد اطلاعاتی و جنگ سایبری و راهکارها، سطوح و ابزارهای مطرح در آن وجود دارد. آنچه مسلم است اینکه در جهان امروز که بر پایه‌ی

رقابت است، همواره احتمال حمله‌ی سایبری به افراد، سازمان‌ها و کشورها وجود دارد. بنابراین لازم است، ابتدا با گسترش پژوهش در این حوزه، زمینه‌ی لازم برای شناخت آن را فراهم آورد. سپس با تدوین سیاست‌ها و راهبردهای لازم، امکان پیشگیری و افزایش توانمندی‌ها را به وجود آورد. همانگونه که نبرد اطلاعاتی در سطوح متفاوتی می‌تواند حادث شود، باید از جنبه‌ها و سطوح متفاوت هم شناسایی شده و تحت کنترل در آید. دولت‌ها نیز باید درک صحیحی از این مفهوم پیدا کرده و در سیاست‌گذاری‌ها و برنامه‌ریزی های خویش به آن بپردازند. همچنین افراد و سازمان‌ها باید ضمن توجه به امنیت اطلاعات خویش، مدیریت اوضاع را در دست گرفته و اطلاعات دستکاری شده و تبلیغات غلط را شناسایی کنند. به نظر می‌رسد مجهز شدن به سلاح اطلاعات، تنها راه پیش‌رو برای کنترل و مقابله با نبردهای اطلاعاتی و جنگ‌های سایبری است.

منابع

منابع فارسی

سلماسی زاده, م. (۱۳۸۰). جنگ اطلاعات و امنیت، *خبرنامه انفورماتیک، ۱۶*، ۲۰ -۲۵.

کاستلز، ا. (۱۳۸۰). *عصر اطلاعات؛ ظهور جامعه شبکه ای*(جلد یک). (ا. خاکباز، مترجم). تهران: نشر طرح نو.

منابع لاتین

Bellamy, C. (1998). *Oxford companion to military history*. Oxford: oxford university press.

Crawford, G. A. (1994). *Information warfare: New roles for information systems in military operations*. Washington DC: Department of the air force.

Crilley, K. (2001). Information warfare: New battlefields terrorists, Propaganda and the Internet, *Aslib Proceedings*, *53*(7), 250-262.

Deborah, R. and Gangemi, G.T. (1994). *Computer security basics*. New York: O'Reilly & Association.

Denning, D. (2000). *Cyber terrorism testimony before special oversight panel on terrorism*, Presented at committee and armed services. US house of representatives Georgetown University, 23th May. Washington DC. , USA.

Dorothy, E. (1999). *Information warfare and security*. Massachusetts: Wesley.

Haeni, R. E. (1997). *Information warfare: an introduction*. Washington DC: Cyberspace Policy Institute.

Herd, G. P. (2003). *Information Warfare & the second chechen campaign*. Retrived from http://www.da.mod.uk/CSRC/documents/CEE/G81/G81.chap6

Hutchinson, W. (2002) .Concepts in information warfare. *Logistics Information Management*, *15*(5/6), 410-413.

Jahangiri, A. (2008). *Cyberspace, Cyberterrorism and information warfare: A perfect recipe for confusion* .Available at: www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

Mc Lendon, C. J. W. (1994). *Information warfare: Impacts and concerns*. Alabama: Maxwell air force base.

Mulvenon, J. (1998). The pla and information warfare. In J. C. Mulvenon & R. H. Yang (Eds.), *The people's liberation* army in the information age, (PP. 175-186). United States, RAND Corporation.

Munro, L . (2009). Defending the network organization: An analysis of information warfare With reference to Heidegger. *SAGE 17*(2), 199–222.

Schwartue, W. (1994). *Information warfare-chaos on the electronic superhighway*. New York: Thounders Mouth press.

Smith, R. (2000). *Simulating information warfare using the HLA management object model*. Orlando. Florida: B. T. G. Inc.

Søndrol, T., Wiehe, A., Sollie, R., Sporild, M., Dahl, O. M., Skarderud, F., Olsen, O.K. (2004). Indicators of information warfare. Retrived from http://www.roarsollie.net/skole/Indicators%20of%20Information%20Warfare.pdf.

Toffler, A. (1993). *War & anti war: Survival at the dawn of the 21st century*. Boston Little Brown and company.

Wilson, C. (2004). *Information warfare and cyberwar: capabilities and related policy issues*. Foreign Affairs, Defense, and Trade Division. Available at: http://www.fas.org/irp/crs/RL31787.pdf .

پی نوشت ها

[1] Clausewitz

[2] Sun Tzu

[3] . Haeni

[4] Smith

[5] Mulvenon

[6] Bellamy

[7] Wilson

[8] Crilley

[9] Denning

[10] Schwartue

[11] Herd

[12] Søndrol

[13] OODA (Observe, Orient, Decide & Art) LOOP

[14] Crawford

[15] Hutchinson

[16] Deborah& Gangemi