فصلنامه مطالعات جنگ
سال دوم، شماره پنجم، تابستان ۱۳۹۹
مقالهٔ سوم از صفحه ٥٤ تا ۷۲

عصر اطلاعات، عصر نوینی از نبرد

عزیز اله محبی گرگری[۱]

دریافت مقاله: ۹۹/۰۲/۱۸ پذیرش مقاله:۹۹/۰۴/۱۲

چکیده

نبرد اطلاعات؛ پدیده‌ی جدیدی نیست و از آغاز جامعه‌ی بشریت وجود داشته است. از زمانی که مردمی وجود داشته‌اند که باهم موافق نبودند، نبرد نیز وجود داشته است. امروز هم ادامه دارد و پایانی برای آن دیده نمی‌شود. کسانی که اطلاعات بهتری دارند و به سرعت و به درستی از آن استفاده می‌کنند، برندگان نبردها هستند. تأثیر این نوع نبرد با افزایش شدید اطلاعات جهانی و فضای سایبری، شدت گرفته است. برای قرن‌ها، رمزنگاری، برای پنهان کردن و آشکار کردن پیام‌ها به کار می‌رفت؛ حتی لغت سی‌فر[۲]، به معنای رمزنگاری از لغت عربی «صفر» به معنای «هیچ» مشتق شده است. امروزه در دوران اطلاعات و داده به سر می‌بریم و بنابراین نبرد اطلاعات هیچ تعجبی ندارد. البته تقریباً همه‌چیز را در مقیاس جهانی آن نگاه می‌کنیم و بنابراین نبرد هم در مقیاسی جهانی دیده می‌شود. در حقیقت، نبرد اطلاعات، نشان می‌دهد که اطلاعات، به‌تنهایی، عرصه‌ای جداگانه، سلاحی بالقوه و هدفی پرمنفعت، محسوب می‌شود. نبردی که مرزهای جغرافیایی در آن معنا ندارد. در این نوع نبرد، شاید بخش نظامی، دیگر نتواند میدان نبرد را کنترل کند. تئوری نبرد اطلاعات بر پایه‌ی قوانین فیزیک، اثر متقابل جوامع، اصول و ابزارهایی است که موجب توانمند کردن فرد برای کسب اطلاعات و برتری بر دشمن می‌شود. نبرد اطلاعات در زمان‌های صلح و جنگ، به کار می‌رود. اساس نبرد اطلاعات از جنگ روانی، فریب و عملیات امنیتی، شکل گرفته است. مقاله حاضر، رویکردهای متفاوت نبرد اطلاعاتی، ویژگی‌ها و اهداف آن را مورد مطالعه قرار می‌دهد.

واژگان کلیدی: نبرد اطلاعاتی، جنگ نوین، فضای مجازی، جنگ سایبری.

۱. دانشجوی دکتری تخصصی الکترونیک، مرکز مطالعات و تحقیقات، منطقه پدافند هوایی شمال غرب، تبریز، ایران.
edu.mandegar@yahoo.com

2. cipher

مقدمه

از عصر حاضر با عناوینی چون عصر دیجیتالی، داده و در کل، عصر اطلاعاتی نام برده می‌شود که در این گستره عظیم، سربازان اینترنتی در دانشکده‌های اینترنتی با کسب آموزش‌های لازم، نبردهای اینترنتی را از طریق ارتباطات شبکه‌ای یا موشواره‌ها و سلاح‌ها و بمب‌های الکترونیکی برعلیه دولت‌های دیجیتالی و اهداف و ارتباطات شبکه‌ای و زیرساخت‌های حیاتی کشورها اجرا می‌نمایند. بنابراین، شبکه‌های متعدد اطلاعاتی و ارتباطی، گرچه از یک منظر، «فرصت» تلقی می‌شود، از منظری دیگر می‌تواند تبدیل به «تهدید» شود؛ چراکه بمانند شهری «بی‌پلیس» است، پس برای ورود به این شهرِ شبکه‌ای و دادوستد با عوامل و عناصر موجود باید تدابیر لازم اندیشیده شود.

«مارک پالمر» از استراتژیست‌های معروف آمریکایی (عضو کمیته خطر جاری[1] و یکی از نوآوران سیاست خارجی ایالات متحده در دولت‌های نیسکون، فورد، کارتر، ریگان، بوش پدر و بوش پسر) است که در خارج از مجموعه دولت به طراحی ابتکارات جدید سیاست خارجی مشغول بود. وی ۱۱ سال در شوروی، یوگسلاوی و مجارستان به‌عنوان دانشجو و دیپلمات زندگی کرده و در زمره متخصصین ایران و آسیای قفقاز محسوب می‌گردید. این چهره برجسته اخیراً در گفت‌وگو با خبرنگار روزنامه آمریکایی نیویورک تایمز، صراحتاً با ایده تهاجم نظامی علیه جمهوری اسلامی ایران مخالفت کرده و اعلام نموده است: «ایران به لحاظ وسعت سرزمینی، کمیت جمعیت، کیفیت نیروی انسانی، امکانات نظامی، منابع طبیعی سرشار و موقعیت جغرافیایی ممتاز در منطقه خاورمیانه و هارتلند نظام بین‌الملل، به قدرتی کم‌نظیر تبدیل شده است که دیگر نمی‌توان با یورش نظامی، آن را سرنگون کرد»؛ بنابراین به زعم «پالمر» و اعضای کمیته خطر جاری، تنها راه سرنگونی نظام جمهوری اسلامی ایران، پیگیری جنگ نرم با استفاده از سه تاکتیک «دکترین مهار»، «جنگ رسانه‌ای» و «ساماندهی نافرمانی مدنی» ممکن می‌باشد. متن این گزارش به‌عنوان «ایران و آمریکا، رهیافت جدید» تنظیم شده است. یکی از راه‌های نبرد اطلاعاتی آمریکا علیه ایران راه‌اندازی سایت‌های اینترنتی و ارایه‌ی نرم‌افزارهای جاسوسی به عوامل وابسته در داخل کشور تا ابعاد مختلف نبرد رسانه‌ای به شکل اثربخش‌تر طراحی و اجرا شود که این خود، نبرد سایبری محسوب می‌شود. که نبرد سایبری، جزء نبرد رسانه‌ای عنوان گردیده است. در پایان این گزارش

1. The committee on the present danger

با منتفی دانستن هرگونه گفت‌وگو و مذاکره مستقیم با مقامات ایرانی آمده است: «گفت‌وگو 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» (مکتب اسلام،۱۳۸٤).

نبرد اطلاعاتی

اصطلاح نبرد اطلاعاتی برای نخستین بار در سال ۱۹۷۵ میلادی مورد استفاده قرار گرفت و کشورهای پیشرفته در زمینه فن‌آوری به اهمیت آن پی بردند و تلاش کردند در زمینه‌های سیاسی، اقتصادی، نظامی و فرهنگی آن را به کار ببرند. در اواخر دهه ۹۰ اصطلاح نبرد اطلاعاتی دامنه وسیع‌تری یافت و به عملیات اطلاعاتی معروف گشت و منظور از آن هرگونه عملیات نظامی یا غیرنظامی با هدف سلطه بر تفکر دشمن بود به گونه‌ای که به دلخواه ما فکر کند و اجرای تصمیم‌هایش منافع ما را تأمین کند و از طرف دیگر ممانعت از اینکه دشمن همانند این عملیات را برعلیه ما به کار ببرد (منیرحجاب،۱۳۸۷). تکوین نبرد اطلاعاتی مستقیماً با پیشرفت‌های سریع در فن‌آوری‌های اطلاعاتی جدید مثل شبکه‌های الکترونیک در طی دو دهه اخیر مرتبط است. در واقع، نبرد اطلاعاتی عبارت است از استفاده از شبکه‌های الکترونیکی برای تخریب یا از کار انداختن و غیرعملیاتی کردن زیرساخت‌های اطلاعاتی دشمن که هم می‌تواند علیه یک جامعه (اهداف غیرنظامی) و هم علیه ارتش یا نیروی نظامی آن جهت‌گیری شود. نبرد اطلاعاتی علیه ارتش یا نیروی نظامی می‌تواند مرکب از جنگ کنترل و فرماندهی، جنگ جاسوسی محور و جنگ الکترونیکی باشد و علیه جامعه و نیروهای غیرنظامی می‌تواند مرکب از نبرد اطلاعاتی و اقتصادی و جنگ روانی، سرقت یا تخریب اطلاعات رایانه‌ای باشد. بنابراین، نبرد اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده است. این انقلاب به دلیل دامنه وسیع و تأثیرات گسترده آن می‌تواند سبک نوینی از نبرد را ارائه نماید. نبرد اطلاعاتی یعنی کاربرد اطلاعات و سیستم‌های اطلاعاتی به‌عنوان یک سلاح در درگیری‌هایی که اطلاعات و سیستم‌های اطلاعاتی یک هدف نظامی مهم به شمار می‌روند.

مارتین لیبیکی، تئوریسین و کارشناس مطرح حوزه‌ی مسائل سایبری و دفاعی اندیشکده‌ی رند و مدیر بخش مطالعات امنیت سایبری دانشگاه نیروی دریایی آمریکا و از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی، 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 می‌شود».

مارتین لیبیکی ضمن وفادارماندن به تعریف کاملاً نظامی از نبرد اطلاعاتی هفت شکل مختلف نبرد اطلاعاتی را به شرح زیر نام می‌برد:

– جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.

– نبرد بر پایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی 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 طرز فکر دوستان، بی‌طرف‌ها و دشمنان استفاده می‌شود. جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.

– نبرد اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.

– جنگ سایبر ترکیبی از همه موارد شش‌گانه بالا.

مگان برنز در سال ۱۹۹۹ با نگرشی کلی، تعریف زیر را ارائه می‌دهد: «نبرد اطلاعاتی طبقه یا مجموع‌هایی از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن‌یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست‌یافته و آن را حفظ می‌کند».

مقصود از نبرد اطلاعاتی، عملیات‌های تهاجمی و تدافعی است که توسط سازمان‌های تشکیلاتی یا فردی با سیاست‌های خاص و اهداف راهبردی برای بهره‌برداری و یا تخریب اطلاعات موجود در رایانه‌ها یا شبکه‌اینترنت و دیگر سیستم‌های اطلاعات شبکه‌ای به کار گرفته می‌شود. نبرد اطلاعاتی یک ویژگی درگیری‌های نظامی است که سامانه‌های اطلاعاتی به طور مستقیم یا غیرمستقیم مورد تهاجم واقع شده یا از آن‌ها دفاع می‌شود تا بدین ترتیب داده‌ها، دانش، باورها یا پتانسیل جنگ‌جویی دشمن افت کرده یا کاملاً نابود شود و در عین حال داده‌ها، دانش، باورها و میل جنگ‌جوئی نیروهای خودی حفظ شود. دایره‌المعارف پدافند روانی و پدافند غیرعامل، پس از معرفی جنگ فرماندهی و کنترل جامع‌ترین تعریف ممکن را برای نبرد اطلاعات ارائه می‌دهد:

«جنگ فرماندهی و کنترل عبارت است از کاربرد یکپارچه امنیت عملیات، فریب نظامی، عملیات روانی، جنگ الکترونیک و تخریب فیزیکی برای تأثیرگذاری، افت کیفیت، یا تخریب توانمندی‌های فرماندهی و کنترل دشمن و در عین حال، حفاظت از توانمندی‌های فرماندهی و کنترل خودی در برابر اقدامات مشابه دشمن. زمانی که هدف اصلی چنین نبردی چیزی بیش از فرماندهی و کنترل و ارتباطات دشمن باشد از اصطلاح عمومی‌تر "نبرد اطلاعاتی" استفاده می‌شود که در سطوح غیرنظامی همچون نبرد دیپلماسی و سیاسی و دیگر اشکال ارتباطات نیز کاربرد دارد» (پایگاه اطلاع‌رسانی سازمان پدافند غیرعامل،۱۳۹۱).

نبرد اطلاعات، استفاده از عملیات فیزیکی یا مجازی برای وادار کردن کشورها، سازمان‌ها و افراد به انجام دادن یا انجام ندادن چیزهایی است که به اهداف بلندمدت و کوتاه‌مدت شما کمک می‌کنند و درعین‌حال ممانعت از رقبایتان برای انجام دادن این کار به وسیله شما بکار می‌رود. درواقع این تعریف چیزهایی بیشتر از حمله به کامپیوترها با کدهای مخرب است. آزمایش لیتموس به این صورت است: اگر اطلاعات برای انجام دادن عملیاتی به‌کار برده شود که با آن دیگری را وادار به کاری کنند که به سود حمله‌کننده باشد، آن عملیات، نبرد اطلاعات است. این تعریف یک تعریف بین‌المللی است که سازمان‌ها، مردم و قابلیت‌ها را در برمی‌گیرد. به دولت‌ها، کارتل‌ها، شرکت‌ها، هکرها، تروریست‌ها و دیگر گروه‌ها و افراد فرصت می‌دهد که سهمی در آنچه مورد حمله قرار گرفته است، داشته باشند. هماهنگ کردن این تعریف با نیازهای این گروه‌ها بستگی به خودشان دارد.

مفهوم شناسی

نبرد اطلاعات به‌طور فزاینده‌ای برای بخش نظامی، جوامع اطلاعاتی و بخش تجاری کشورها، اهمیت پیدا کرده است. جیمزدردریان[1]، مدیر مرکز مطالعات بین‌المللی امنیت در استرالیا، در سال ۲۰۰۳، اعلام کرد نبرد اطلاعات، به‌عنوان چتری برای فهم متون جنگ سایبری، جنگ هکرها، جنگ شبکه، جنگ مجازی و سایر حوزه‌های درگیری با محوریت شبکه‌های اینترنتی و فن‌آوری اطلاعات، محسوب می‌شود. در بسیاری از این متون، فن‌آوری و ابزار دیجیتال، با یکدیگر ترکیب شده و به نوع خاصی از فن‌آوری رایانه، اشاره شده است. مطلبی که وجود دارد این است که در متون یادشده، میان نبردهای جدید با نبردهای سنتی، اتصال برقرار شده است. سؤالی که مطرح می‌شود این است که درگیری و نبردها، شامل جنگ‌های روانی نیز می‌شود. مثلاً اگر گروهی یک دستگاه خودپرداز را هک کند، خسارات مالی کمی ممکن است متوجه افراد

1. James Der Derian

شود، ولی آثار روانی آن، می‌تواند برای طولانی مدت، باقی بماند. در این حالت، دیگر مردم، رغبت چندانی به استفاده از این دستگاه‌ها ندارند، هرچند امن‌سازی کامل آن‌ها صورت گرفته باشد. وی گفت: نظریه‌ی اجتناب از رویارویی مستقیم و طولی و رو در رو با دشمن و به دست گرفتن ابتکار عمل دشمن برای ضربه زدن، نشان‌دهنده‌ی هنر نبرد است. نبرد اطلاعات، متشکل از ایده‌ی درگیری جامعه‌ی اطلاعاتی و تهدیدات است. نبرد اطلاعات یعنی استفاده از اطلاعات یا فن‌آوری اطلاعات طی یک بحران یا کشمکش به‌منظور دستیابی به اهداف موردنظر؛ اما جنگ سایبری، حمله به شبکه‌های الکترونیک است. دانشگاه پنسیلوانیا در مورد نبرد اطلاعات گفته است: «هر اقدامی برای انکار، تخریب، فاسد کردن اطلاعات دشمن و عملکرد آن باشد یا هر رفتاری برای حفاظت خود در برابر این‌گونه اقدامات». دن‌کوئل[1]، استاد دانشگاه دفاع ملی واشنگتن، در تعریف نبرد اطلاعات گفته است: «درگیری با تلاش میان دو یا چند گروه در محیط اطلاعات» (علیزاده، ۱۳۹۶).

اطلاعات: در اینجا به معنی محتوا یا معنی یک پیام است. هدف از نبردها، همیشه تأثیرگذاری بر سیستم‌های اطلاعاتی دشمن بوده است. در معنای گسترده‌تر، سیستم‌های اطلاعاتی دربردارنده نوعی وسیله یا شیوه‌ای هستند که بدان طریق بتوان به آگاهی یا اعتقادات خاصی دست پیدا کرد؛ در معنای محدود آنکه سیستم‌های اطلاعاتی، مجموعه‌ای کامل از دانش، اعتقادات و فرایندهای تصمیم‌گیری دشمن هستند. نتیجه مطلوب نیز، آن خواهد بود که دشمن پیام‌هایی را دریافت کند که او را به توقف نبرد متقاعد سازد (عبدالله‌خانی،۱۳۸۶، ص۴۴-۴۵).

نبرد[2]: مجموعه‌ای از تمام فعالیت‌های مهلک و غیرمهلک است که برای غلبه بر اراده حریف یا دشمن انجام می‌شود. در این معنا وارفِیر[3] مترادف وار[4] و نیازمند اعلام جنگ نیست و در عین حال با شرایطی که وضعیت جنگی نامیده می‌شود، همراه نمی‌گردد. نبرد می‌تواند از سوی گروه‌های دولتی، گروه‌های مورد حمایت دولت یا گروه‌های غیردولتی، یا بر ضد آن‌ها صورت گیرد. هدف از نبرد، لزوماً کشتن دشمنان نیست بلکه فقط مهم تحت کنترل درآوردن آنان است (عبدالله‌خانی،۱۳۸۶، ص۴۶-۴۷).

انواع و اشکال نبرد اطلاعاتی

در حالت کلی، نبرد اطلاعاتی به دو نوع مستقیم و غیرمستقیم، است (علیزاده،۱۳۹۶):

- نبرد اطلاعات مستقیم: در این نوع نبرد، اطلاعات دشمن تغییر پیدا می‌کند، بدون اینکه دخالتی در کارکردهای تحلیلی و ادراکی، صورت بگیرد.

---

1. Dan Kuehl
2. Warfare
3. Warfare
4. War

– نبرد اطلاعات غیرمستقیم: در این نوع نبرد، اطلاعات دشمن از طریق دخالت در کارکردهای تحلیلی و ادراکی دشمن، تغییر پیدا می‌کند.

در هر حال، می‌توان نبرد اطلاعات را به اشکال زیر نیز دسته‌بندی نمود:

نبرد فرماندهی و کنترل[1]: هدف آن قطع ارتباط بین ساختار و فرماندهی دشمن از بدنه زیرفرمانش است (لابیکی،۱۳۸۵، ص۹۲). از این نوع جنگ با نام C4I نیز نام برده شده که از چهار C به معنای فرماندهی، نظارت و کنترل، رایانه و ارتباطات شکل می‌گیرد (عبدالله‌خانی،۱۳۸٦، ص۱۲۵)؛ که خود به دو صورت انجام می‌شود.

– هدف قراردادن سرفرمانده[2]: در گذشته همواره این نوع عملیات بر حذف فیزیکی فرماندهی عالی نبرد متمرکز بوده و به طور کلی حذف آن‌ها تأثیرات قابل توجهی بر نتایج نبرد داشته است. امروزه علاوه بر اهمیت نقش فرماندهان، مراکز فرماندهی به‌عنوان مؤلفه‌ی بسیار مهم این نوع عملیات، ایفای نقش می‌کند. حمله به یک مرکز فرماندهی به‌ویژه اگر به‌موقع انجام گیرد، می‌تواند حتی بدون زدن یک فرمانده عالی‌رتبه دشمن، عملیات را مختل کند (عبدالله‌خانی، ۱۳۸٦، ص۱٤٦).

– هدف قرار دادن گردن فرمانده[3]: این عملیات علیه خطوط ارتباطی و اطلاعاتی فرماندهی و بخش‌های مختلف صحنه‌ی عملیات صورت می‌گیرد. قطع این ارتباط الکترونیکی، منجر به ضعف و شکست می‌شود (عبدالله‌خانی،۱۳۸٦، ص۱۲٦).

نبرد اطلاعات محور (نبرد مبتنی بر اطلاعات عملیات)[4]: این نوع نبرد زمانی رخ می‌دهد که اطلاعاتی به گونه‌ای مستقیم، عملیات‌ها را (به خصوص در تعیین هدف و ارزیابی خسارت‌های نبردی) هدایت کند، به جای اینکه اطلاعات به‌عنوان یک داده به فرماندهی و کنترل منتقل و مورد استفاده قرار گیرد این نبرد منجر به کاربرد مستقیم فولاد (بمب) علیه دشمن می‌شود (به جای اینکه بایت‌ها را خراب کند) (لابیکی،۱۳۸۵، ص۹٦). این نبرد در دو محور انجام می‌شود.

– نبرد اطلاعات‌ـ محور آفندی (نبرد تهاجمی)[5]: افزایش سریع قدرت در مقایسه با قیمت فن‌آوری‌های اطلاعاتی، به‌ویژه فن‌آوری‌های سیستم‌های پخش متمرکز، طرح‌های جدیدی را برای

---

1. Command and control warfare
2. Antihead
3. Antineck
4. Intelligence Based Warfare (IBW)
5. Offensive IBW

جمع‌آوری و پخش اطلاعات عرضه می‌کند محیط نبردهای آینده دارای حس‌گرهای گوناگونی خواهد بود که به طور کامل میدان نبرد را نشان می‌دهند، بدین ترتیب فرمانده می‌تواند طرح‌ها و برنامه‌های نبرد را اجرا کند (لابیکی،۱۳۸۵، ص۹۷-۹۸).

- نبرد اطلاعات- محور پدافندی (نبرد تدافعی)[1]: در اینجا آنچه مهم است ایجاد روش دفاعی به‌منظور افزایش شکاف میان تصویر و واقعیت در میدان نبرد است؛ یعنی کاری کنیم که حس‌گرهای دستگاه‌های جمع‌آوری اطلاعات دشمن، یا به اطلاعاتی نرسند یا اگر رسیدند منطبق با واقعیت نباشد (عبدالله‌خانی،۱۳۸٦، ص ۱۲۹).

نبرد الکترونیکی[2]: برای کاهش دادن ارتباطات، چه در سطح فیزیکی (از طریق پارازیت در رادارها یا مخابرات) و چه در سطح ترکیبی (به‌وسیله ره‌گیری یا حقه زدن) انجام می‌شود.

نبرد روانی[3]: استفاده از اطلاعات برعلیه ذهن و فکر افراد و انسان‌ها

نبرد نفوذگر[4]: حمله هکرها به سیستم‌های اطلاعاتی نظامی و امنیتی

نبرد اطلاعاتی اقتصادی[5]: از راه تحریم اطلاعاتی حاصل می‌شود به‌طوری که بتوان با تحریم اطلاعات، موانعی را در تجارت و اقتصاد آن کشور هدف ایجاد کرد البته امکان فیزیکی تجارت، از بین نمی‌رود (لابیکی،۱۳۸۵، ص۱۰۸-۱۰۰).

نبرد سایبر یا اینترنتی[6]: استفاده از رایانه و اینترنت برای نبرد در فضای سایبر

نبرد ادراکی: عملیات‌هایی که به‌منظور تاثیرگذاری بر عقاید و رفتار مردم، از رسانه‌های جمعی در دسترس آن‌ها سوءاستفاده می‌کنند. جنگ ادراکی هدفی مشابه عملیات روانی دارد اما حوزه عمل آن از حوزه عملی عملیات روانی گسترده است (عبدالله‌خانی،۱۳۸٦، ص۱۳۳).

کاربردهای نبرد اطلاعاتی

کاربردهای نبرد اطلاعاتی را در عرصه نظامی می‌توان به‌صورت زیر خلاصه کرد (صدوقی،۱۳۸۰، ص۱۳۷):

---

1. Defensive IBW
2. Electronic Warfare
3. Psychological Warfare
4. Hacke warfare
5. Economic Information warfare
6. Cyber warfare

آمادگی: مدیریت یکپارچه در صحنه نبرد (آمادگی درگیری شدید در صحنه نبرد، حمله در زمان مناسب و تدارک به موقع).

پدافند: جلوگیری از قطع ارتباطات رایانه‌ای در صحنه نبرد.

آفند: سعی در قطع ارتباطات رایانه‌ای در حوزه فرماندهی، نظارت، ارتباطات رایانه‌ای و جمع‌آوری اطلاعات، مراقبت و شناسایی دشمن.

ابزارهای نبرد اطلاعاتی

ویروس‌ها: ویروس‌ها برنامه‌هایی می‌باشند که قادر به تکثیر خود به برنامه‌های بزرگ‌تر هستند. برنامه‌های ویروس، وقتی فعال می‌شوند که برنامه میزبان شروع به فعالیت کند و دنبال آن ویروس، خود را تکثیر می‌کنند و برنامه‌های دیگر را آلوده می‌نمایند. ویروس‌ها در هر محیط رایانه‌ای ساخته می‌شوند. پس تعجب‌آور نیست که به مثابه جنگ‌افزار اطلاعاتی مورد استفاده قرار بگیرند. وقتی یک عامل ویروس‌های رایانه‌ای را به داخل شبکه‌های رایانه‌ای رخنه داده باشد، در آن حالت شبکه هدف از کار می‌افتد و یا حداقل نارسایی‌های وسیعی در آن‌ها ایجاد می‌شود.

کرم‌ها: کرم‌ها یک برنامه مستقل است که به طور شعله‌ور خودش را تکثیر می‌کنند و از یک رایانه به رایانه‌ای دیگر و اغلب بر روی شبکه‌ها حرکت می‌کند و برخلاف ویروس‌ها، برنامه‌های دیگر را تغییر نمی‌دهد. پیامدهای مخرب این جنگ‌افزار دو زمینه قابل بررسی است: یکی نابودی منابع موجودی اطلاعاتی در شبکه و دیگری تغییر شکل و انتشار در شبکه.

اسب تروا: اسب‌های تروا برنامه‌هایی هستند که در داخل سایر برنامه‌ها پنهان می‌گردند و برنامه خود را به اجرا درمی‌آورند. اسب تروا می‌تواند خود را استتار کند و حتی در برنامه‌های ایمنی شبکه مانند SATAN قرار بگیرند.

بمب منطقی: بمب منطقی یک نوع اسب تروا‌ست که برای آزاد کردن ویروس‌ها یا سیستم‌های تهاجمی دیگری استفاده می‌شوند و می‌تواند به‌صورت یک برنامه مستقل که توسط برنامه‌نویس و طراح در سیستم جاسازی می‌شود، عمل کند. نظر به این‌که تعداد زیادی نرم‌افزار از امریکا صادر می‌شود، از طرف دولت امریکا، پیشنهاد شده است که در هر نرم‌افزار صادراتی اسب تروا نصب شود. این عامل مخفی می‌تواند در شرایطی که آن کشور علیه امریکا وارد نبرد شد، از راه دور فعال شده و اثرات مخرب آن می‌تواند شامل فرمت کردن دیسک سخت و ارسال اسناد به سازمان سیا باشد (صدوقی، ۱۳۸۰، ص ۱۳۱–۱۳۰).

درهای پشتی یا دامی: این شامل سازوکارهایی است که طراح نرم‌افزار در زمان ساخت نرم‌افزار تعبیه می‌کند تا در زمانی که سیستم حفاظت رایانه به طور طبیعی کار می‌کند به طراح امکان می‌دهد تا به طور مخفیانه وارد سیستم شود. این مکانیزم در زمان نبرد اطلاعاتی قادر است سیستم‌ها و اطلاعات ذخیره شده در کشورهای خارجی را مورد کاوش و جست‌وجو قرار دهد. این مهمترین مسئله و برنامه‌ریزی در استراتژی نظامی و منبعی برای فراهم آوردن اطلاعات حیاتی برای بخش جاسوسی است.

تخریب چیپ‌ها: همانطور که نرم‌افزار می‌تواند کارهای غیرمنتظره انجام دهد، می‌توان همان کارکرد را درون سخت‌افزار تعبیه کرد. چیپ‌های امروزی شامل میلیون‌ها مدار مجتمع می‌باشد که سازنده آن به راحتی می‌تواند در آن‌ها تغییر شکل دهد و همچنین قادر است کارهای غیرمنتظره انجام دهند. چیپ‌ها می‌توانند بعد از زمان خاصی از کار بیافتند یا بعد از رسیدن علائمی منفجر شوند و یا امواج رادیویی از خود صادر کنند که باعث تعیین دقیق محل آن‌ها شود.

میکروب‌ها: این‌ها می‌توانند باعث تخریب‌های شدید در سیستم‌ها بشوند و برخلاف ویروس‌ها می‌توانند بر روی سخت‌افزار و نه نرم‌افزار مؤثر واقع شوند. با توجه به این‌که میکروب‌هایی وجود دارند که نفت می‌خورند این پرسش‌ها وجود دارد که آیا می‌توان آن‌ها را برای خوردن ماده سلسیم پرورش داد؟ در صورت عملی بودن، می‌توان پیش‌بینی کرد که بتوان کلیه مدارهای مجتمع را تخریب کرد.

اختلالات الکترونیکی: استفاده از اختلالات رایانه‌ای برای سد کردن ارتباطات و در مرحله پیشرفته، دادن اطلاعات غلط و بیش از حد.

بمب‌های EMP و تفنگ‌های HERF: HERF امواج رادیویی با قدرت زیاد است که می‌تواند امواج رادیویی پرقدرت را به اهداف الکترونیکی شلیک کند و آن‌ها را از بین ببرد. تخریب این وسیله می‌تواند کم شدت باشد و فقط موجب خاموش شدن و روشن شدن مجدد آن گردد و باعث صدمه به سیستم سخت‌افزاری (به طور فیزیکی) شود. اهداف آن می‌تواند یک مین‌فریم در داخل یک ساختمان یا کل یک شبکه در داخل ساختمان باشد. حتی هدف می‌تواند یک وسیله متحرک باشد که به تجهیزات الکترونیک مجهز است (لابیکی،۱۳۸۵، ص۱۳۲-۱۳۱).

پالس‌های الکترومگنتیک: منبع آن می‌تواند انفجارات هسته‌ای و یا غیرهسته‌ای باشد و می‌تواند توسط نیروهای ویژه‌ای که داخل منطقه دشمن نفوذ کرده‌اند در نزدیک مراکز الکترونیک منفجر

شود و باعث تخریب قسمت‌های الکترونیک تمام رایانه‌ها و سیستم‌های مخابراتی در منطقه کاملاً وسیع شود (لابیکی،۱۳۸۵، ص۱۳٤-۱۳۲). این پدیده که در آغاز به‌عنوان اثر جنبی آزمایش‌های هسته‌ای کشف شد. اکنون به مولدهای غیرهسته‌ای گسترش یافته است این مولدها می‌توانند یک EMP ایجاد نمایند که سیستم‌های الکترونیکی حافظ را ناتوان سازد. این بمب‌ها خساراتی را بوجود می‌آورند که دائمی است (عبدالله‌خانی،۱۳۸٦، ص۱٤۲).

سطوح نبرد اطلاعاتی

سطح تاکتیکی: شکل‌های سنتی حملات اطلاعاتی مانند اقدامات ضد رادار در حوزه فرماندهی، نظارت، ارتباطات، نیز رخنه کامپیوتری و عملیات روانی است که از ویژگی‌های زیر برخوردار می‌باشد:

– روش‌های اقدام و ضد اقدام: اهداف، منطقه‌ای هستند و دورنمای محدودی دارند و صرفاً در یک عملیات رزمی خاص قابلیت هماهنگی وجود دارد.

– از فعالیت‌های نظامی پشتیبانی می‌کند: این شکل از حملات در سطح تاکتیکی انجام می‌شود و نیاز به دانستن مشخصات تکنیکی و روش‌های عملیاتی دارد و می‌تواند در قالب چند عملیات هم‌زمان و پی در پی انجام شود. در اینجا، صحنه نبرد گسترش می‌یابد و از محدوده مرزهای جغرافیایی و زمانی در زمان صلح، بحران یا صحنه نبرد گسترش می‌یابد. در حالت کلی، تاکتیک‌های نبرد اطلاعات شامل تشخیص مسئله، تحریف حقایق، منحرف کردن اذهان، دلسرد کردن مردم می‌باشد (علیزاده،۱۳۹٦).

سطح استراتژیک: جنگ‌افزارهای استراتژیک نبرد اطلاعاتی به طور گسترده‌ای باعث کاهش اهمیت فاصله و مسافت می‌شوند، به‌طوری که آسیب‌پذیری‌های C3I در میدان نبرد، اهمیت کمتری از آسیب‌پذیری‌های زیرساخت‌های غیرنظامی ملی پیدا می‌کند. اصولاً هدف نهایی این رویارویی، روند تصمیم‌گیری رقیب و دشمن است (صدوقی،۱۳۸۰، ص۱۳٤-۱۳۳). در تعریف گسترده مشترک از نبرد اطلاعاتی، اهداف واقعی نبرد اطلاعاتی صرفاً بر روی سیستم‌های تهاجمی دشمن متمرکز نمی‌باشند، بلکه بر روی روندهای تصمیم‌گیری دشمن طراحی می‌شود. به همین دلیل، باید گفت که طراحی حملات نبرد اطلاعاتی بر اساس مشخصات سیستم‌های تهاجم نیست بلکه، بر پایه تأثیرگذاری در سطوح بالای فرماندهی است؛ مثلاً در یک عملیات جنگ الکترونیک، حملات اختلالی علیه حس‌گرها بر اساس دانستن مشخصات تکنیکی و عملیاتی حس‌گرها

می‌باشد، در حالی که در جریان حمله نبرد اطلاعات، طراحی و هدایت آن علیه اطلاعاتی که حس‌گرها از وضعیت منطقه برای نیروهای تهاجم به دست می‌آورند، مدنظر می‌باشد (صدوقی، ۱۳۸۰، ص ۱۳۰).

ویژگی نبرد اطلاعاتی

کم‌هزینه بودن ورود به نبرد اطلاعاتی: داشتن تخصص در سیستم‌های اطلاعاتی و شبکه‌های الکترونیکی یا داشتن متخصص در این زمینه و دسترسی به شبکه‌های الکترونیکی از شرایط لازم مهم برای ورود به این قسم از نبرد می‌باشد (صدوقی،۱۳۸۰، ص۱۳٦-۱۳٤). ساز و برگ نبرد اطلاعاتی برای پیشبرد از نبرد با بسیج شهروندان نیاز دارد و نه به بسیج منابع، به جای آن فقط به جذب لبه‌های پیشرو نوآوری‌های صنعتی برای مقاصد تکیه می‌کند مثل مهندسی الکترونیک، کامپیوتر، مخابرات، هوافضا و غیره (وبستر و کوین،۱۳۸٤، ص۲۲۲).

فناوری فوق‌العاده پیچیده: ساز و برگ نبرد اطلاعاتی با استفاده از فناوری‌های فوق‌العاده پیچیده هدایت می‌شود.

انعطاف‌پذیری: به دلایل گوناگون، ساز و برگ نبرد اطلاعاتی به برنامه‌ریزی نیاز دارد، اما این برنامه‌ریزی برای پاسخی انعطاف‌پذیر است برای نبردی که تحرک، انعطاف‌پذیر و واکنش سریع را در اولویت قرار می‌دهد. برنامه‌ریزی ازقبل، به خاطر چنین پیچیدگی در برنامه‌ریزی برای انعطاف‌پذیری است که بسیاری از جنبه‌های ساز و برگ نبرد اطلاعاتی را از پیش برنامه‌ریزی می‌کنند و از آن طریق دست جنگ‌جویان واقعی را کوتاه می‌سازند (وبستر و کوین،۱۳۸٤، ص۲۲۳-۲۲۲).

خدشه در مرزبندی‌های سنتی: متعدد بودن مخالفان و دشمنان احتمالی، تنوع در جنگ‌افزارها و گوناگونی استراتژی‌ها موجب می‌شود که شناسایی منابع تهدید در این نبرد به طور فزاینده‌ای با مشکلات فراوانی رو به رو شود، به‌طوری که اغلب اوقات با دشواری می‌توان بین منابع داخلی و خارجی تهدیدهای نبرد اطلاعاتی تفاوت و تمایز قایل شد. حتی نمی‌توان به راحتی دریافت که چه کسی مورد حمله قرار گرفته و چه کسی متهم به حمله کردن است، مرز بین زمان صلح و نبرد به طور فزاینده‌ای کدر می‌شود.

افزایش اهمیت و نقش دست‌کاری: در نبرد اطلاعاتی این امکان وجود دارد تا با تکیه بر تکنیک‌های اطلاعاتی، توانایی فریب و دست‌کاری را افزایش داد.

مشکلات سخت هشدار تاکتیکی و ارزیابی حمله: در حال حاضر هیچ‌گونه سیستم هشدار دهنده تاکتیکی با کفایتی که قادر باشد بین حملات استراتژیک نبرد اطلاعاتی و دیگر انواع فعالیت‌های ارتباطات رایانه‌ای نظیر جمع‌آوری اطلاعات یا حوادث اتفاقی تمایز ایجاد می‌کند، وجود ندارد. نتیجه آنکه نمی‌توان تشخیص داد که دقیقاً چه زمانی حمله می‌شود، از کجا حمله می‌شود، چه کسی حمله می‌کند و تهاجم چگونه هدایت می‌شود.

چالش جدید جاسوسی: در جهان سایبر، جایی برای پنهان شدن وجود ندارد. با افزایش ماهواره‌های متصل به شبکه‌های الکترونیکی توان مراقبت الکترونیکی بی‌نهایت افزایش می‌یابد.

دشواری ایجاد و نگهداری ائتلاف: متعدد بودن مخالفان و دشمنان احتمالی که می‌توانند به‌صورت فردی نیز ظاهر شوند و تنوع در جنگ‌افزارها و استراتژی‌ها و کاهش توانایی پیش‌بینی متحدان و دشمنان، ایجاد ائتلاف و نگهداری آن را با مشکل فزاینده‌ای روبرو می‌کند (صدوقی، ۱۳۸۰، ص۱۳٦-۱۳٤).

اهداف نبرد اطلاعاتی

هدف نبرد اطلاعات، به دست آوردن قدرت برای تسلط به دیگران، قدرت و نفوذ در قلب چنین روابطی است. نبرد اطلاعات نیاز به تلاش دارد و تلاش، نیاز به کسب قدرت برای رسیدن به سود اقتصادی یا تسلط نظامی در میدان نبرد یا بازار دارد. از طرفی، هدف نبرد اطلاعات، برتری اطلاعاتی و امن‌سازی سامانه‌های اطلاعاتی در برابر دشمن یا هدف مورد نظر است؛ اما جنگ سایبری (به‌عنوان گونه‌ای از نبرد اطلاعات) می‌تواند چنین تعریف شود: «نبردی با فناوری‌های بالا در بستر فضای سایبری». اصولاً این نوع، بر پایه‌ی ماشین‌ها است. به‌عنوان مثال می‌توان در این راستا از شناسایی ماهواره‌ها به‌عنوان جنگ سایبری، نام برد. در حقیقت برخی ابعاد جنگ سایبری را می‌توان، جزو نبرد اطلاعات، قلمداد کرد. مثلاً اگر حمله سایبری به مرکزی صورت بگیرد و هدف آن، تغییر اطلاعات یا حذف اطلاعات باشد، قطعاً این حملات، زیرشاخه نبرد اطلاعات است (علیزاده،۱۳۹٦). اهداف نبرد اطلاعاتی را می‌توان در سه لایه از هم متمایز کرد که در هر لایه یک پیامد خاص ایجاد می‌شود:

لایه سیستم اطلاعاتی: این سطح شامل عناصر مادی، تولید، انتقال و ذخیره می‌باشد و حملات علیه سیستم‌های اطلاعاتی باعث ایجاد پیامدهای تکنیکی می‌شود.

لایه مدیریت اطلاعاتی: در این سطح روندهای پردازش اطلاعات و مدیریت آن مورد حمله قرار می‌گیرد و باعث ایجاد پیامدهای کارکردی می‌شود.

لایه تصمیم‌گیری: این سطح مربوط به تصمیم‌گیری و استفاده از اطلاعات در امر تدوین و تنظیم سیاست و تصمیمات است. حملات در این سطح، می‌تواند پیامدهای عملیاتی ایجاد کند (صدوقی، ۱۳۸۰، ص۱۳٦).

فرق نبرد اطلاعاتی و جنگ با فن‌آوری و تسلیحات پیشرفته

استفاده از شبکه‌های الکترونیکی برای اهداف مزیت اطلاعاتی بخش عظیمی از نبرد اطلاعاتی را تشکیل می‌دهند. اصطلاح نبرد اطلاعاتی که روز به روز استفاده از آن گسترده‌تر می‌شود اغلب به اشتباه جنگ با فن‌آوری و تسلیحات پیشرفته که ارتش‌های بزرگ و پیشرفته از آن استفاده می‌کنند، اشتباه گرفته می‌شود. در حالی که باید توجه داشت از فن‌آوری اطلاعاتی پیشرفته در زمینه بالا بردن دقت، افزایش برد و تقویت قدرت کشندگی سلاح‌های متعارف استفاده می‌شود، اما در نبرد اطلاعاتی هیچ کدام از این عناصر کاربرد ندارند. نبرد اطلاعاتی صرفاً به اطلاعات و داده‌ها که در قالب ذرات الکترونیک شناخته می‌شوند، محدود نمی‌گردد. حتی تخریب فیزیکی مبادلات مخابرات نیز نبرد اطلاعاتی محسوب نمی‌شود، اما از کارانداختن سیستم سوئیچینگ تلفن‌ها با ویروس، نبرد اطلاعاتی نامیده می‌شود.

اصولاً، نبرد اطلاعاتی نتیجه ظهور جامعه اطلاعاتی است که هنوز در بسیاری از کشورها معمول نشده است. در جوامع اطلاعاتی تمامی مبادلات اجتماعی، اقتصادی، سیاسی و فرهنگی ماهیتاً دیجیتال و البته وابسته به رایانه شده‌اند؛ یعنی در جامعه اطلاعاتی بیشتر اتفاقات معنادار، بین افراد و سازمان‌ها باواسطه رایانه‌ها و شبکه‌های رایانه‌ای صورت می‌پذیرد. وضعیت در این جوامع به گونه‌ای است که مقادیر زیادی از اطلاعات سیستم‌های پیچیده شامل شهرها، بازارهای مالی، بهداشت، ثروت و ذخایر، تولید و حتی توزیع را در داخل خود جای داده‌اند (صدوقی،۱۳۸۰، ص۱۳۰-۱۲۹).

دفاع اطلاعاتی[1] یا امنیت اطلاعات[2]

دفاع اطلاعاتی: عبارت است از فرایند شناسایی و تحلیل اطلاعاتی که برای عملیات‌های نیروهای خودی حیاتی می‌باشد و شامل موارد زیر است (پایگاه اطلاع‌رسانی سازمان پدافند غیرعامل،۱۳۹۱):

– شناسایی اطلاعاتی که سامانه‌های اطلاعاتی دشمن می‌توانند آن را مشاهده نمایند.

– تعیین شاخص‌هایی که نشان می‌دهد سامانه‌های اطلاعاتی مهاجم چگونه اطلاعات حیاتی را در زمان مناسب برای بهره‌برداری نیروهای دشمن استخراج می‌کنند.

– گزینش و اجرای اقداماتی که آسیب‌پذیری برای اقدامات نیروهای خودی را در برابر سوء استفاده نیروهای دشمن از بین برده یا کاهش می‌دهند.

امنیت اطلاعات: هیچ انسانی بدون امنیت نمی‌تواند به ادامه‌ی حیات خود امیدوار باشد؛ چه در دنیای واقعی و 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. در واقع، امنیت اطلاعات به معنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز است. این فعالیت‌ها عبارت‌اند از دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر، دست‌کاری (کرمی کامکار،۱۳۹۱).

مفاهیم اصلی امنیت اطلاعات

اطلاعات در تعریف علمی، به مجموعه‌ای از داده‌ها که دارای معنی و هدف باشند اطلاق می‌شود. ازاین‌رو، اطلاعات می‌تواند به هر نوع از داده‌های معنی‌دار نظیر اطلاعات چاپی، کاغذی، الکترونیکی، صوتی و تصویری گفته شود و حتی گفته‌های شفاهی ما به یکدیگر را نیز پوشش دهد. موارد سه‌گانه حفظ درستی، محرمانگی و دسترس‌پذیری از مفاهیم اصلی امنیت اطلاعات است (کرمی کامکار،۱۳۹۱).

– درستی (یکپارچه بودن): یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دست‌کاری غیرمجاز اطلاعات.

– محرمانگی: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز.

---

[1]. Information Defense

[2]. Information security

– قابل دسترس بودن: اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند.

کنترل امنیت اطلاعات

کنترل امنیت به اقداماتی گفته می‌شود که منجر به حفاظت، پیشگیری، مقابله یا واکنش و به حداقل رساندن دامنه تهدیدات امنیتی در صورت بروز می‌شود. این اقدامات را می‌توان به سه دسته تقسیم نمود (کرمی کامکار،۱۳۹۱).

– مدیریتی: کنترل مدیریتی (کنترل رویه‌ها) عبارت‌اند از سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول تأیید شده است.

– منطقی: کنترل منطقی (کنترل فنی) استفاده از نرم‌افزار، سخت‌افزار و داده‌ها برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های رایانه‌ای است.

– فیزیکی: کنترل فیزیکی برای حفاظت و کنترل محیط کار و تجهیزات رایانه‌ای و نحوه دسترسی به آن‌ها است که جنبه فیزیکی دارند. به‌عنوان مثال: درب، قفل، گرمایش و تهویه مطبوع، آژیر دود و آتش، سیستم دفع آتش‌سوزی، دوربین‌های مداربسته، موانع، حصارکشی، نیروی‌های محافظ و غیره.

پس از اقدامات اولیه امنیت اطلاعات می‌توان شناسایی اطلاعات موردنظر، شناسایی کاربرد اطلاعات شناسایی شده، تعیین کارهای مجاز و غیرمجاز روی آن اطلاعات با توجه به کاربردهای شناسایی شده را نام برد.

خط‌مشی امنیت اطلاعات[1]

طبق این استاندارد، پس از شناخت انواع اطلاعات و کاربردها و اهداف آن‌ها باید خط‌مشی امنیت در سازمان تعیین شود. خط‌مشی به ما می‌گوید:

– حفاظت از کدام دسته از اطلاعات سازمان برای ما مهم‌تر است؟

– ما باید خود را برای چه نوع ریسک‌هایی آماده کنیم؟

– چه خطراتی درستی، محرمانگی و در دسترس بودن اطلاعات سازمان ما را تهدید می‌کند؟

– کارهای پیشنهادی ما برای پیشگیری یا واکنش در برابر این خطرات کدام‌اند؟

[1]. Information Security Policy

ساختار امنیت اطلاعات

ایجاد یک ساختار برای امنیت اطلاعات کمک می‌کند تا پاسخ سؤال‌های زیر را بیابیم.

– چه ساختار سازمانی برای اداره روش‌های امنیت اطلاعات لازم است؟

– چه کمیته‌هایی باید تشکیل شود و چه مسئولانی باید تعیین شوند؟

– آیا از مشاوران و صاحب‌نظران برای کمک در امور تخصصی استفاده می‌شود؟

– بازبینی‌های دوره‌ای برای اطمینان از روش‌های درست امنیت اطلاعات توسط چه کسانی و در چه دوره‌هایی انجام می‌شود؟

– سیاست‌های سازمان برای برخورد با افراد بیرونی و پیمانکاران در ارتباطات با اطلاعات سازمان چیست؟

چالش امنیت اطلاعات

یکی از چالش‌های بزرگ امنیت اطلاعات، نیروی انسانی در هر شرکت یا سازمانی هست، در این زمینه باید مواردی را کنترل کنیم. آیا افراد سازمان کارهای مجاز و غیرمجاز امنیتی را می‌شناسند و از تبعات آن‌ها آگاه‌اند؟ آیا آن‌ها از گزارش‌دهی در مورد وقایع امنیتی اطلاعات (نظیر خطاهای نرم‌افزاری، نقص‌های امنیتی، ویروس‌ها و غیره) را یاد گرفته‌اند؟ آیا کارکنان به لحاظ امنیت اطلاعات، مورد پذیرش قرار می‌گیرند؟ چه سطحی از گزینش برای هر شغل لازم است؟ آیا برای کارکنان تازه و کم‌تجربه، آموزش‌های خاص در ارتباط با امنیت اطلاعات در نظر گرفته می‌شود؟

دسترسی به اطلاعات همواره می‌تواند موجب بروز مشکلات امنیتی شود؛ بنابراین، مؤلفه‌هایی باید به روشنی تعریف شده باشد: ثبت کاربران، مدیریت سطوح دسترسی کاربران، مدیریت و کاربرد اسامی رمز، بازنگری حقوق دسترسی کاربران، امنیت تجهیزات کاربر در غیاب کاربر، کنترل مسیرهای شبکه‌ای، اعتبارسنجی کاربران در اتصال از خارج از شبکه، اعتبارسنجی دستگاه‌های کاری، حفاظت درگاه‌های دسترسی از راه دور، جداسازی شبکه‌ها، کنترل اتصالات شبکه‌ای، کنترل مسیریابی شبکه‌ای، امنیت خدمات شبکه، روش ورود به سیستم عامل، شناسایی و اعتبارسنجی کاربر، محدودیت در زمان و مدت اتصال کاربر به شبکه، جداسازی سیستم‌های حساس.

پیشنهاد یک راه‌کار

می‌توان گفت پازل رسانه‌ای آمریکا، انگلیس و متحدانش، برای تحت فشار قراردادن انقلاب اسلامی ایران طراحی شده و راه‌کار خنثی‌سازی و بی‌اثرکردن تلاش‌های دشمنان، ایجاد فضای هم‌نوایی و هم‌گرایی بین نیروهای درون نظام و عمل به مقتضیات اتحاد ملی به‌عنوان رهیافت راهبردی نظام انقلاب اسلامی است.

افشای حقایق و اوضاع داخلی آمریکا، انگلیس و متحدانش و نیز برملا نمودن توطئه‌های غرب در آسیای غربی و جهان اسلام و نیز تقویت زمینه‌های «انسجام ملی» در زمره‌ی راه‌کارهایی هستند که می‌توانند در ناکامی نقشه‌های مراکز راهبرد سازی دولت‌های بیگانه و متحدان آمریکا در ایجاد نبرد اطلاعاتی علیه انقلاب اسلامی ایران تأثیرگذار باشند.

نتیجه‌گیری

نبرد اطلاعاتی یک توانمندی استراتژیک است مانند تسلیحات هسته‌ای در زمان جنگ سرد که عامل تهدید و یا تهدید پذیری یک کشور محسوب می‌شود. ازنظر استراتژی کاربردی، نبرد اطلاعاتی معتقد است که بجای تسلیحات با حجم تخریب زیاد باید تسلیحات دقیق علیه نقاط حساس را بکار برد. درنتیجه برتری اطلاعاتی را می‌توان در قدرت پردازش اطلاعات دانست. نداشتن آمادگی در نبرد اطلاعاتی، شبیه ملت بدون ارتش و قوای نظامی است. امروزه، سرمایه‌گذاری در نبرد اطلاعات «انتخابی» نیست و دولت‌های دارای دفاع ضعیف در برابر فضای اطلاعاتی، مجبور به تسلیم هستند؛ که در واقع، نادیده گرفتن نبرد اطلاعاتی، مقدمه حمله نظامی است. نبرد اطلاعاتی در واقع یکی از پرکاربردترین ابزارهای «نبردهای میدانی» است که آمریکا و متحدانش در این حوزه از طریق شبکه‌های رسانه‌ای و ارتباطاتی خود، توانسته‌اند به یکی از بازیگران تأثیرگذار این نبرد جدید تبدیل شوند. هدف نبرد اطلاعات، کنترل و نفوذ بر عملکرد تصمیم‌گیران است. منطقه‌ی کنترلی، می‌تواند مستقیماً دست‌کاری شود در حالی که منطقه‌ی نفوذ، تنها به‌صورت غیرمستقیم قابل دسترسی است. کنترل و نفوذ، عصاره‌ی قدرت هستند. از دیدگاه تجاری و صنعتی، داشتن بیشترین سهم بازار و سود، امکان انجام بهتر نبرد اطلاعاتی را فراهم می‌کند. نبرد اطلاعات، یکی از شیوه‌های نوین جنگ و از مهم‌ترین ابزار نفوذ به افکار و تغییر راهبردها است.

فهرست منابع:

- نشریه مکتب اسلام، ۱۳۸۴، شماره (۳). کلیپ جنگ نرم و دشمن شناسی سایت aja.ir، کد خبر: ۱۸۰۲۲۰.
- منیرحجاب، محمد؛ ۱۳۸۷؛ جنگ روانی (الحرب النفسیه)، تهران؛ مرکز آموزشی و پژوهشی شهید صیاد شیرازی.
- پایگاه اطلاع رسانی سازمان پدافند غیرعامل کشور، ۱۳۹۱، دفاع اطلاعاتی: جنگ اطلاعات، کدخبر: ۷۷۵، ۱۹ آذر ۱۳۹۱.
- علیزاده، بابک. ۱۳۹۶، مقدمه‌ای بر جنگ اطلاعات، سایبر نیوز، ۱۰ تیر ۱۳۹۶.
- عبدالله خانی، علی؛ ۱۳۸۶؛ جنگ نرم ۳ (نبرد در عصر اطلاعات)، تهران. موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.
- لابیکی، مارتین ک؛ ۱۳۸۵؛ هفت نوع جنگ اطلاعاتی؛ گزیده‌ای از عصر اطلاعات (الزامات ملی در عصر اطلاعات)، دیوید س آلبرتس، دانیل س پاپ؛ علی علی‌آبادی، رضا نخجوانی؛ تهران؛ پژوهشکده مطالعات راهبردی.
- صدوقی، مرادعلی؛ ۱۳۸۰؛ تکنولوژی اطلاعاتی و حاکمیت ملی، تهران، وزارت امور خارجه.
- وبستر، فرانک؛ کوین، رابینز؛ ۱۳۸۴؛ عصر فرهنگ فناورانه (از جامعه اطلاعاتی تا زندگی مجازی)، ترجمه: مهدی داودی؛ تهران؛ توسعه.
- کرمی کامکار، محمدرضا. ۱۳۹۱، امنیت اطلاعات چیست؟، پورتال رسمی شرکت فناوران حفیظ سامانه، کد مقاله ۳۰، ۱۳۹۱/۳/۲۲.