

اطلاعات و جنگ اطلاعات

(Information & Information warfare)

ترجمه: علی نیازی
ویرایش: بیژن مرادی

چکیده

از اواخر قرن بیستم پدیده جدیدی ناشی از انقلاب در امور نظامی (RMAs)^۱ به نام جنگ اطلاعات (IW)^۲ در وزارت دفاع و ستاد نیروهای مسلح به ویژه کشورهای پیشرفته نظامی مطرح شده، و امروزه یکی از مباحث مهم در حوزه دفاعی و غیر دفاعی کشورها است. شاید بتوان گفت ظهور این تفکر با تحول اطلاعات و گسترش این باور که این تحول می‌تواند چهره جدیدی از جنگ مدرن باشد، ارتباط مستقیم داشته باشد. توسعه روز افزون فناوری ارتباطات و اطلاعات، و استفاده گسترده از آن در امور روزمره عمومی و نظامی، فضایی به وجود آورده که می‌تواند منابع ملی یک کشور که به طور عمده خارج از میدان‌های نبرد نظامی قرار دارند را به شدت به خطر اندازد. این مقاله به اهمیت جنگ اطلاعات، موج‌های مختلف جنگ، عوامل مؤثر، تعاریف و اهداف جنگ اطلاعات، و در پایان به تقسیم بندی حوزه های هفت گانه جنگ اطلاعات می‌پردازد.

^۱. Revolution in military affairs

^۲. Information warfare

مقدمه

پیش بینی می شود جنگ اطلاعات در آینده گونه ای جدید از جنگ باشد. گرچه اهمیت اطلاعات از زمان های گذشته نیز شناخته شده بود، ولی امروزه جنگ تا حد بی سابقه ای مبتنی بر سامانه های اطلاعاتی است. سامانه های جمع آوری اطلاعات، نظیر ماهواره های شناسایی و هشدار دهنده سریع و مجموعه وسیعی از سامانه های هوایی با سرنشین یا بدون سرنشین، مقادیر زیادی اطلاعات فراهم می نمایند که از طریق رابط های (link) پیشرفته مخابراتی توزیع می شوند. این سامانه ها، از یک سو باعث افزایش توانایی رزمی نیروها می شوند و از سوی دیگر به طور بالقوه آسیب پذیرند. در نتیجه، هدف در این حوزه از جنگ، کاربرد مؤثر منابع اطلاعاتی خودی و در عین حال تخریب یا از کار انداختن منابع اطلاعاتی دشمن می باشد. یک بررسی کلی نشان می دهد که امکان استفاده از سامانه های اطلاعاتی به تنهایی می تواند به عنوان ابزاری برای مختل کردن زیر ساخت های اطلاعاتی نظامی و غیرنظامی به کار رود. به هر حال نیروهای متخصص در جنگ های آینده از ابزارهای اطلاعات و سایر سامانه های اطلاعاتی جهت دستیابی به برتری در فضای نبرد استفاده خواهند کرد. و شاید روزی اهمیت یک ریزتراشه (chip) الکترونیکی مجتمع در یک رایانه، بسیار مفید تر از اثر تخریب فیزیکی یک تن اورانیم روی اهداف دشمن باشد.

امروزه با وجود تفاسیر و تعاریف متعددی که از جنگ اطلاعات شده است، هنوز این پدیده به صورت یک معما باقی مانده است. کشورهای دارای فناوری برتر به مقدار قابل توجهی در آزمون این جنگ هزینه نموده اند. ضمن اینکه شناخت کلی بر این است که پتانسیل خدمات رسانی آن به عنوان یک نیروی مهم چند برابر کننده قدرت است، اما تدابیر کلی در گام های اولیه و بسیار مقدماتی اش است. در نهایت اینکه در قرن حاضر موفقیت جنگ اطلاعات به عنوان عنصری از قدرت امنیت ملی، بستگی به نوعی معماری جنگ اطلاعات ماندگار و معتبر دارد.

موج های مختلف جنگ

صاحب نظران نظامی از جنگ اطلاعات به عنوان موج سوم جنگ نام برده، و این پدیده را ناشی از سیر تکامل و پیشرفت فناوری اطلاعات دانسته اند. و به طور کلی سیر تکامل جنگ را با موج های زیر مشخص نموده اند:

موج اول جنگ بر پایه توانایی جامعه کشاورزی با هدف دستیابی به زمین، و ابزارهای آن محدود به سلاح هایی بود که انرژی آن را ماهیچه های انسان فراهم می نمود.

موج دوم جنگ مربوط به دوران انقلاب صنعتی با هدف دستیابی به منابع و تولیدات صنعتی صورت گرفت، نوع جنگ افزارهای آن استاندارد شده و در قالب تولید انبوه بود و همگام با تولید انبوه کشتار جمعی نیز در برداشت.

موج سوم جنگ بر دانش، اطلاعات و بر پایه اصول اقتصاد استوار است، هدف آن دستیابی و کنترل آگاهی و اطلاعات می باشد.

انهدام و تخریب ساختار فرماندهی و کنترل عراق و استفاده از جنگ افزارهای دقیق در عملیات طوفان صحرا نمونه ای از موج سوم جنگ است.

عوامل رویکرد به جنگ اطلاعات:

عامل اول، شناخت و تشخیص اطلاعات به عنوان ابزاری راهبردی برآورد شده، به طوری که طراحان نظامی با دسترسی مجدد به آن به پویایی میدان نبرد نایل گردند.

عامل دوم، تجارب و آزمون هایی بود که از عملیات طوفان صحرا گرفته شد که در آن موفقیت کارآیی و توانمندی جنگ افزارها نشان داد (مانند سلاح های هدایت شونده دقیق).

عامل سوم، پیشرفت در فناوری اطلاعات، توانمندی و کاربرد بالقوه آن در میدان نبرد است.

عامل چهارم، رشد فناوری تجاری و آسیب پذیری های مرتبط با یکپارچگی این فناوری در داخل نیروهای مسلح است.

ترتیب توالی اطلاعات

داده خام (raw data):

پایین ترین طبقه اطلاعات (information)، و شامل سیگنال های خامی است که

توسط حسگرها (سنسورها) از هر طریقی مانند (آنتن گیرنده، چشم، رادار و ماهواره) یا هر گونه وسیله ارتباطی دیگری دریافت می شوند. داده خام، سیگنال‌هایی هستند که هنوز در فرایند تفسیر، توازن، تقاطع و ارزیابی قرار نگرفته‌اند و به همین لحاظ به ندرت قابل بهره برداری می باشند زیرا مفهوم معنی داری ندارند.

داده یا داده ها (data) :

گروه دوم اطلاعات، که در فرایند پردازش قرار داده شده، یا در قالب و شکلی قرار دارد که برای کاربران آن دارای مفهوم است. مثل فیلم منفی که به عکس تبدیل شده، یا متنی که روی صفحه رایانه نمایان می شود.

آگاهی (knowledge) :

در این مرحله، داده (data) تجزیه و تحلیل می شود تا معنا و ارزش پیدا کند. آگاهی یعنی داده ارزیابی شده ای که قابلیت اعتماد و اطمینان یافته، مرتبط باشد و درجه اهمیت آن نیز مشخص گردد.

آگاهی، داده های پردازش شده ای هستند که یکپارچه و تفسیر گردیده اند تا تصویری از وضعیت میدان نبرد را ارائه دهند. برای مثال، اطلاعات نظامی شکلی از آگاهی می باشند که با اخبار رزمی (combat information) که هنوز در فرآیند تجزیه و تحلیل قرار نگرفته است، مقایسه می شوند.

درک (understanding):

بالاترین رده سلسله مراتب اطلاعاتی، درک "understanding" است، یعنی آگاهی "knowledge" که ترکیب، هماهنگ و به یک وضعیت خاصی تبدیل گردیده تا درک عمیق تری از هشیاری "awareness" وضعیت میدان نبرد را ارائه دهد (تصویر ذهنی کاملی از وضعیت).

درک به مفهوم رسیدن به "هشیاری از وضعیت" یعنی آشکار شدن نقاط حیاتی یک وضعیت، و یا به عبارتی آشکار شدن نقاط ضعف و آسیب پذیری های حساس و حیاتی دشمن.

تعاریف جنگ اطلاعات

در مقدمه کتاب جنگ اطلاعات اثر ن. شوارتز^۱، ج. آلگر^۲ (رئیس مدرسه جنگ اطلاعات در دانشگاه دفاع ملی آمریکا)، جنگ اطلاعات بدین صورت تعریف شده است:

"اعمالی که به قصد حفاظت، بهره برداری، تخریب، تکذیب و یا انهدام اطلاعات و منابع آن جهت دستیابی به برتری قابل ملاحظه و یا پیروزی بر دشمن انجام می گیرد."

وزارت دفاع آمریکا در سال ۱۹۹۶ جنگ اطلاعات را چنین تعریف نموده است. " عملیات اطلاعاتی که در طول یک بحران و یا جنگ برای دستیابی و یا به نمایش گذاشتن برتری بر دشمن یا دشمنان انجام می گیرد. " " عملیات اطلاعاتی اعمالی هستند

¹ Nin Schwartaus

² John Alger



که بر اطلاعات و سامانه های اطلاعاتی دشمن تأثیر گذاشته و به دفاع از اطلاعات و سامانه های اطلاعاتی خودی می پردازند." وجه مشترک تمام تعاریف ارائه شده به سه جنبه زیر تمایل دارند:

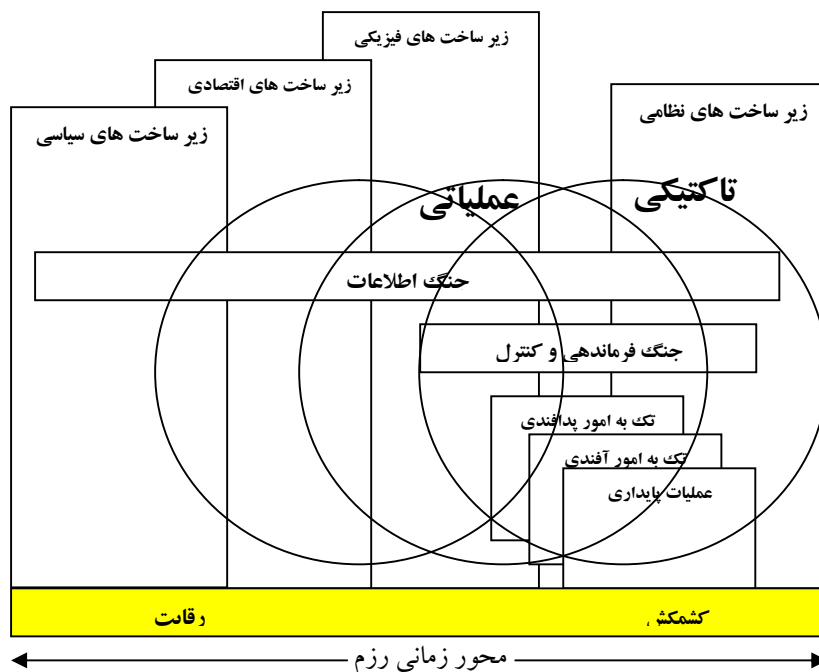
حفاظت سامانه های اطلاعات خودی در برابر اقدامات و آینده های اطلاعاتی دشمن

تک یا حمله به سامانه های اطلاعاتی دشمن

بهره برداری از سامانه های اطلاعاتی طرف متخاصم با هدف بهره برداری از امتیازات و ویژگی های عملیات اطلاعاتی.

پ- اهداف جنگ اطلاعات

جنگ اطلاعات اثرات دوربرد و دیر زمانی دارد همانگونه که در شکل ۱ دیده می شود، جنگ اطلاعات فقط شامل اهداف نظامی متداول نمی گردد بلکه امور سیاسی و زیرساخت های جامعه را مورد هدف قرار می دهد. برای مثال کشور چین پی برده که کشورهای ابرقدرت مانند آمریکا را نمی تواند با قدرت هسته ای فعلی مورد تهدید قرار دهد، اما با استفاده از جنگ اطلاعات می تواند ثبات مالی آنها را در زمان صلح به خطر اندازد.



شکل ۱ - معماری جنگ اطلاعات

جنگ اطلاعات، طیف گسترده ای از فعالیت ها را تحت تأثیر قرار می دهد، اما به طور کلی شامل اقداماتی می گردد که بازیگران عرصه نبرد اطلاعات، با ابزارهای رایانه ای قادر به نفوذ در رایانه ها، شبکه های رایانه ای و سامانه های اطلاعاتی حریف می گردند؛ این گونه نفوذها می توانند پیامدهایی نظیر: اختلال در هدایت هواپیماها، کنترل نیروگاه ها و سایر سامانه هایی که بر روی شبکه های همگانی و اختصاصی به تبادل اطلاعات می پردازند را به همراه داشته باشند. در جنگ اطلاعات، تهاجم بدون سروصدا و در سکوت محض آغاز می گردد، اثری از آژیرهای هشدار دهنده بمباران هوایی و صدای انفجار موشک

های دوربرد مشاهده نمی‌شود. شهروندان هم به طرف پناهگاه‌ها هجوم نخواهند برد. در این گونه نبردها، رایانه‌ها و مراکز کنترل نیروگاه‌ها از کار خواهند افتاد. خاموشی سرتاسر منطقه عملیات را فرا می‌گیرد، سامانه‌های راداری فرودگاه‌ها و پایگاه‌های هوایی غیرفعال می‌شوند. سامانه‌های کنترل ترافیک و راه‌های کشور تعطیل، خطوط تلفن قطع و ایجاد ارتباط در کل منطقه تحت پوشش جنگ اطلاعات، غیر ممکن می‌شود، شبکه‌های اینترنتی غیرقابل دسترس شده و پیام‌های شبکه‌های صدا و سیما قابل دریافت نخواهند بود. جنگ اطلاعات در سکوت محض و بدون وجود علائم متعارف از جانب کشور یا گروه متخاصم اجرا و به دنبال آن، نگرانی و اضطراب شهروندان آغاز می‌شود. در این شرایط دشمنی با هویت نامعلوم، با استعداد و آرایش نظامی نامشخص و همچنین موقعیت جغرافیایی ناشناخته، می‌تواند وارد کشور شده، مناطق حساس مورد نظر خود را فتح کند.

در جنگ اول خلیج فارس، انواع مختلف عملیات جنگ اطلاعات به نمایش گذاشته شد، مواردی همچون نفوذ به رایانه‌ها، اطلاعات عملیاتی (intelligence)، جاسوسی ماهواره‌ای، شنود رادیویی، پایش و نظارت پیرامونی، جنگ الکترونیک، تخریب فیزیکی تجهیزات ارتباطی، فریب از طریق اطلاعات جعلی، مدیریت افکار، عملیات روانی و ویروس‌های رایانه‌ای نمونه‌هایی از جنگ اطلاعات بودند. البته موارد دیگری نظیر

سرقت اسرار تجاری، رخنه به منابع بخش خصوصی، جعل نامه های الکترونیکی و از این قبیل نیز جزو عملیات جنگ اطلاعات محسوب می گردند و بسته به شرایط، برخی از آنها جرم به حساب می آیند، بعضی از آنها در صورتی که غیر اخلاقی نباشند، غیرمتعارف محسوب نمی شوند. برخی از انواع عملیات نفوذ رایانه ای از نظر دولت ها قابل قبول هستند و برخی دیگر در شرایط نبرد بخشی از ابزارهای نظامی محسوب می شوند، اما فصل مشترک همه آنها دسترسی به منابع اطلاعاتی یا تخریب آنها به منظور کسب برتری است.

حوزه های جنگ اطلاعات:

در یک دیدگاه کلی، جنگ اطلاعات به هفت حوزه زیر تقسیم می شود:

۱- جنگ فرماندهی و کنترل (C2W) ۲- جنگ مبتنی بر سامانه های هوشمند

- ۳- جنگ الکترونیک
- ۴- جنگ روانی
- ۵- جنگ اطلاعات اقتصادی
- ۶- جنگ نفوذگری
- ۷- جنگ سایبری

نتیجه گیری:

با توجه به این که پدیده جنگ اطلاعات به عنوان یکی از مباحث مهم در حوزه دفاعی و غیر دفاعی مطرح است و می تواند منابع ملی کشورها را، که به طور عمده خارج از میدان های نبرد نظامی قرار دارند به خطر اندازد و وقوع جنگ های اخیر در منطقه نیز مؤید این واقعیت می باشد، بنابراین ضروری است سیاست گذاران و برنامه ریزان نظامی و غیرنظامی کشور، با برنامه ریزی های درازمدت و کوتاه مدت، فرهنگ سازی و اختصاص بودجه مورد نیاز، آموزش های کاربردی را در نیروهای مسلح ایجاد و همزمان مسئولین دولتی نیز زیرساخت های مورد نیاز را برای عملیات آفندی و پدافندی جنگ اطلاعات فراهم نمایند تا آمادگی لازم برای مقابله با تهدیدات بالفعل و بالقوه در زمینه جنگ اطلاعات به طور مطلوب و در تمامی ابعاد فراهم گردد.

مرجع:

1. Information Warfare-National Defense University
2. Defining information power-N.D.U strategic forum