

جنگ اطلاعاتی در جنگ نامتقارن

چکیده:

تحولات عصر اطلاعات آنچنان سریع و شتابان رخ می‌دهد که تحلیل دقیق آن دشوار و بررسی و شناخت آن ضروری است. یکی از این عرصه‌ها، حوزه جنگ است. جنگ اطلاعاتی که خود ناشی از ظهور و بروز و فراگیری فناوری اطلاعات است به سرعت میدان‌های متفاوت را درنوردیده و حوزه جنگ‌ها را نیز از خود متأثر ساخته است. از سوی دیگر جنگ کلاسیک نیز در پرتو تغییرات حوزه‌های قدرت و فناوری، چهره‌های جدیدی از جنگ را تجربه کرده که جنگ نامتقارن یکی از آنهاست. از آنجا که این شیوه جنگ می‌تواند طرف‌های ضعیف‌تر و کوچک‌تر را در تحمیل اراده برطرف قوی‌تر، کارآمد سازد به سرعت مورد توجه کانون‌های قدرت و بازیگران عرصه‌های سیاست و جنگ قرار گرفته است. به همین منظور بررسی آخرین پیامدهای فناوری اطلاعات درحوزه جنگ یعنی جنگ اطلاعاتی و تأثیرات آن بر آخرین تحولات در قلمرو جنگ یعنی جنگ نامتقارن اهمیت ویژه یافته و این تعامل مورد بررسی اندیشمندان قرار گرفته است. در این مقال مختصر از باب درآمدی بر گشودن بحث‌های نوین، این تأثیر و تأثر مورد بحث و کنکاش قرار گرفته است.

کلید واژه‌ها: جنگ war، جنگ اطلاعاتی *Information warfare*، جنگ

نامتقارن *Asymmetric warfare*، تهدیدات نامتقارن *Asymmetric Threats*.

مقدمه

شاید بتوان گفت که جنگ، ناخوشایندترین پدیده تمدن بشری است. نزاع و کشمکش میان مخلوقات دیگر خداوند نیز وجود دارد ولی برای انسانها که اشرف مخلوقاتند و خلقت آنها با پدیده عقل، تکمیل گردیده است، نمی تواند پدیده ای میمون و مبارک باشد.

با این حال، همواره جنگ در مقاطع تاریخی متفاوت، سرنوشت تمدن های گوناگون را رقم زده است. جنگ ممکن است کوتاهترین راه برای تحمیل اراده بر دشمن باشد ولی هیچ گاه بهترین آنها نبوده است. با وجود این، همواره با آن رو به رو هستیم و برای دفاع در برابر چنین پدیده ای تنها باید آمادگی های خویش را افزایش دهیم.

جنگ در طول تاریخ چهره های گوناگونی را از خود نشان داده است چه از نظر خشونت و چه از نظر شیوه های تسلط و چیرگی. این تجربه ها امروزه در اشکال گوناگون تکرار می گردد. جنگ و گریزها، حملات تهاجمی نظامی کلاسیک، حملات شبه نظامی، چریکی، تروریستی و گونه های مختلف آنها تجربیاتی را به وجود آورده است که باید بتوانیم با بهره برداری از آنها استراتژیها و تاکتیکهایی را شکل دهیم که از آسیب پذیری های گذشته کاسته و بر توان کنونی خود بیفزاییم.

تحولات دو قرن اخیر در غرب و پیشرفت های شگفت آور فناوریهای نوین همان گونه که چهره زندگی انسانها را تغییر داده، تحولات جدی را در صحنه های کشمکش و نزاع به وجود آورده است. هر یک از حوزه های نوین فناوری خود به سهم خویش در تغییر این شیوه ها و روشها مؤثر بوده اند.



رخداد فناوری اطلاعاتی^۱ با ویژگی‌های خاص خویش بیش از هرچیز دیگری، در تحولات اخیر تاثیرگذار بوده و به همراه تحولات فناوری، انقلابی را در امور نظامی^۲ به وجود آورده که پدیده جنگ را دچار دگرگونی جدی گردانیده است. از سوی دیگر تفاوت سطوح قدرت موجب گردید که قدرتمندان برای تحقق خواسته‌های خود بیش از هر چیز به اعمال قدرت تکیه کنند و از ره‌آورد این اعمال قدرت، مطامع زورمندانه خود را محقق نمایند؛ اما داستان در اینجا پایان نمی‌پذیرد. کشورها، گروه‌ها و سازمانهای کوچکتر با بهره‌برداری از پیامدهای پیشرفت فناوری به سراغ پاشنه‌های آشیل زورمندان رفته و آنها را در نقاط آسیب‌پذیر خود مورد تهاجم قرار داده‌اند. رفته رفته این پدیده‌ها با هم تنیده شده‌اند و پیچیدگیهای بسیاری را در جنگ و تهاجم و دفاع به وجود آورده‌اند که دیگر نمی‌توان به راحتی بر قدرت کلاسیک تکیه زد و از ره‌آورد پیشرفتهای شگفت‌آور تسلیحاتی و تجهیزاتی، سرنوشت همه رؤیایها را پیش بینی نمود. انقلاب اطلاعات^۳ از یک سو انقلاب در امور نظامی را به وجود آورد و از سوی دیگر جنگ را در حوزه اطلاعات گسترش داد و سیستم‌های کنترل و فرماندهی را در صحنه تاکتیک‌ها مورد تهاجم قرار داد و سیستم‌های زیر ساختی را در سطح استراتژیک و در قلب کنترل اطلاعاتی آسیب‌پذیر نمود. جنگ‌ها با تغییر شکل رو به رو گردیدند و نبردهای نامتقارن^۴ از جدیدترین و نوظهورترین اشکال آن برای بسیاری از ابرقدرتها و قدرتهای برتر، کابوسهایی وحشتناک را به وجود آورده‌اند.

۱ - *information Technology (IT)*

۲ - *Revolution in Military Affaris (RMA)*

۳ - *Information Revolution (IR)*

۴ - *Asymmetric warfares*

در این نوشتار مختصر بر آنیم تا از تعامل جنگ اطلاعاتی^۱ و جنگ نامتقارن سخن بگوییم و آخرین تغییرات این صحنه‌ها را در حوزه‌های تأثیر و تأثر مورد بحث قرار دهیم تا بتوانیم نیم رخ از این تحولات را در عرصه جنگ در برابر چشمان تیزبین پژوهشگران و دوستداران اندیشمند قرار دهیم.

جنگ اطلاعاتی

جنگ اطلاعاتی از پیامدهای اصلی و اساسی انقلاب اطلاعاتی و از نتایج تأثیر و تأثر فناوری اطلاعات و حوزه‌های نظامی، دفاعی و امنیتی است. بدین سبب باید نخست از ویژگی‌های فناوری اطلاعات سخن بگوییم و سپس از رویداد انقلاب اطلاعات و جنگ اطلاعاتی و میدانها و حوزه‌های این جنگ بحث نماییم.

در تعاریف اولیه و مقدماتی، جنگ اطلاعاتی را «تهاجم به اطلاعات و زیر ساخت‌ها و سامانه‌های پایه‌ای اطلاعاتی دشمن در ضمن حفظ اطلاعات سامانه‌های اطلاعاتی خودی»، تعریف کرده‌اند. با اندک تأملی در این تعریف می‌توان به خوبی دریافت که این جنگ که در حوزه‌های اطلاعاتی و سیستم‌های اطلاعاتی با دشمن رخ می‌دهد، از یک سو کاملاً صبغه تهاجمی دارد و از سوی دیگر در عین تهاجم، به تدافع و حفظ سیستم‌های اطلاعاتی و اطلاعات خودی نیز تاکید می‌کند.

از آنجا که اطلاعات از دیرباز در امور نظامی نقش اساسی بازی می‌کرده است و اطلاعات در حوزه‌های عملیاتی و تاکتیکی جنگ تأثیری بسزا داشته است، لاجرم فرماندهان و تصمیم گیرندگان براساس اطلاعات به دست آمده حرکت می‌کرده‌اند و می‌کوشیده‌اند تا با نوعی تفوق و برتری اطلاعاتی بر دشمن خود چیره گردند. از همین مرحله بود که در حوزه اطلاعات، مقوله‌ای به نام «برتری اطلاعاتی» مطرح گردید این امر تاکنون ادامه یافته و به طور روزافزونی بر اهمیت آن افزوده شده است.

^۱ - *information warfare (IW)*



در این نوشتار به این نکته بسنده می‌شود که نمی‌توان در هیچ یک از اشکال و انواع جنگ از اهمیت اطلاعات غفلت نمود. باید بر این نکته نیز تأکید کرد که در شیوه‌های پیچیده‌تر جنگ و در جنگ‌های نوین امروزی، جنگ اطلاعاتی به شیوه‌ای از جنگ و نوعی از تهاجم تبدیل شده است. با این رویکرد باید یادآور شد که هنگام سخن گفتن از جنگ اطلاعاتی در جنگ نامتقارن، در واقع از جنگی درون جنگ دیگر یا به عبارت دیگر از جنگ در جنگ سخن گفته می‌شود.

جنگ اطلاعاتی در میدانهای نبردی رخ می‌دهد که می‌توان آن را، فضای رایانه‌ای یا سایبری^۱ نام نهاد. ویژگی‌های این میدان‌های نبرد، شرایط خاصی را بر این جنگ تحمیل نموده و تمایز جدی با دیگر جنگ‌ها به وجود آورده است. جنگ اطلاعاتی در سطوح مختلف و حوزه‌های گوناگون اطلاعات رخ می‌دهد. در سطح استراتژیک، جنگ اطلاعاتی استراتژیک^۲ را به وجود می‌آورد و در سطح عملیاتی جنگ اطلاعاتی را در سطح فرماندهی و کنترل^۳ و در سطح میدانهای نبرد، جنگ اطلاعات تاکتیکی^۴ را شکل می‌دهد. شکل و شیوه‌های جنگ کلاسیک و سنتی، اطلاعات را در حوزه جنگ اطلاعات انسانی بیشتر متمرکز می‌کرد و در جنگ‌های مدرن تکیه جنگ بیشتر بر جنگ الکترونیک^۵ متمرکز گردید و امروز در جنگ‌های پست مدرن، جنگ در حوزه‌های رایانه‌ای رخ می‌دهد. به عبارت دیگر جنگ‌های پست مدرن در پایگاههای اطلاعاتی صورت می‌گیرد.

۱- *Cybery space*

۲- *Strategic information warfare*

۳- *C4I (operational information warfare)*

۴- *tactical information war*

۵- *Signal intelligence (sigint)*

با توجه به این نکته می‌توان روش‌های پیچیده جنگ اطلاعاتی را در انواع جنگ‌های پست مدرن مورد بررسی قرار داد. امروزه جنگ نامتقارن با تمام پیشینه‌های خود، نوعی جنگ پست مدرن محسوب می‌گردد و در کلیه آثار و ادبیات این موضوع، از این جنگ به عنوان نوعی جنگ مدرن یا پست مدرن نام برده می‌شود. از این رو جنگ اطلاعاتی در سامانه‌های رایانه‌ای می‌تواند به پیامدهای بسیار سنگین و سهمگین‌تری منجر گردد که در جنگ‌های سنتی تنها در سطح تلفات انسانی قابل مقایسه و سنجش می‌باشد.

جنگ اطلاعاتی در سیستم‌های اطلاعاتی با تکیه بر حرکت‌های اطلاعاتی در فضای سایبری، صورت می‌گیرد. جنگجویان این میدان‌های نبرد، متخصصان و کارشناسان فعال در حوزه‌های سایبری هستند. امروزه برخی از این جنگجویان را با نام‌های «هکر» معرفی می‌کنند. هر چند هکرها صرفاً در این حوزه‌های جنگی به کار گرفته نمی‌شوند ولی می‌توان گفت هکرها حرفه‌ای شبیه مزدوران در جنگ‌های سنتی عمل می‌کنند. با وجود این اکنون بسیاری از کشورها و سازمان‌های درگیر در جنگ‌های اطلاعاتی، خود هکرها را پرورش و تربیت می‌کنند. در این مرحله بهتر است با تبیین جنگ اطلاعاتی در سطوح مختلف، به کارکردهای جنگ اطلاعاتی در جنگ نامتقارن بپردازیم.

در این مقاله به بحث پیرامون جنگ اطلاعاتی در حوزه نظامی و دفاعی پرداخته می‌شود و سپس در پیوندی با جنگ نامتقارن از این جنگ بحث خواهید شد.

ویژگی‌های جنگ اطلاعاتی

جنگ اطلاعاتی در حوزه‌های نظامی، از فعالیت‌های اطلاعاتی در مدارهای اطلاعاتی در جنگ آغاز می‌شود. نخست باید این نکته را یادآور شویم که در سیستم‌های سنتی آنچه به شکل داده یا خبر بر یک مدار اطلاعاتی وارد می‌گردد پس از ارزیابی



به دانسته‌ها تغییر پیدا می‌کند و سپس با طی کردن یک فرایند هوشمندانه سازمان می‌یابد و به اطلاعات منتجه تبدیل می‌شود.

همواره باید در نظر داشته باشیم که دانسته‌ها پس از تحلیل، به اطلاعاتی تبدیل می‌شود که نیازهای مصرف‌کنندگان را برآورده می‌نماید. این مدار در اثر تحولات ناشی از فناوری اطلاعاتی و انقلاب اطلاعاتی به سیکلی تبدیل گردیده که پیوسته اطلاعات منتجه نیز خود می‌توانسته در طی این فرایند، به عنوان داده‌های اولیه مورد استفاده قرار گیرد و اطلاعات تولید شده دیگری را برای مصرف‌کنندگان به وجود آورد. لذا در سیستم‌های اطلاعاتی که پس از انقلاب اطلاعاتی به وجود آمد، مدار اطلاعاتی دوسویه گردید.

این وضعیت تنها می‌تواند زمانی ایجاد شود که قدرت پردازش اطلاعات و ایجاد ارتباطهای منطقی بین داده‌ها و دانسته‌ها در عرض زمانی بسیار کوتاه رخ دهد. این موقعیت را فقط می‌توان در فضای سایبری تصوّر کرد و سپس آنچه را تصوّر می‌شود، محقق گردانید. روشن است که اطلاعات به دست آمده در چنین سیستمی قابل مقایسه با اطلاعات داده شده در مدار یک سویه قبلی نیست. با توجه به این تحول و با نظر به رخداد چنین وضعیتی در مداری که کلیه مفاصل آن با سیستم‌ها و سامانه‌های رایانه‌ای هدایت و کنترل گردیده است می‌توان دریافت که جنگ اطلاعاتی در فضای شبکه‌ای چگونه می‌تواند هم به تخریب اطلاعات و هم به بهره‌برداری منجر گردد و چگونه در چنین فرایندی ممکن است از آسیب‌پذیری‌های دشمن بتوان با تخصیص حداقل منابع، حداکثر بهره‌برداری را نمود.

با توجه به اینکه چنین وضعیتی می‌توانست از برتریهای بسیار بالایی برخوردار باشد، خود به خود تمامی سیستم‌های اطلاعاتی پیشرفته با به کار گرفتن رایانه‌ها و ابررایانه‌ها چنین فضایی را شکل داد و از طریق اتصال به شبکه جهانی، مدار بسیار پر قدرت و

پیچیده‌ای را فراهم کرد که این مدار در کل جهان گسترده گردید و هر لحظه به جمع‌آوری، ارزیابی، تحلیل و تولید اطلاعات آن افزوده شد. از یک سو کشورهای پر قدرت و ابر قدرت که خود مبدع چنین وضعیتی بودند، از بهره‌مندیهای اطلاعاتی بسیار بالایی برخوردار شدند و از سوی دیگر آرام آرام خود را در برابر تهدیداتی یافتند که در صورت تحقق، ضربات و صدمات بسیار سنگینی را باید تحمل می‌نمودند. بدین ترتیب جنگ اطلاعاتی در مراحل ذیل در چنین مواردی شکل گرفت:

مراحل جنگ اطلاعاتی

الف) نفوذ^۱

ب) بهره‌برداری^۲

ج) تخریب اطلاعات^۳

د) انهدام سامانه‌های اطلاعاتی^۴

هـ) انهدام زیرساختهای حیاتی و حساس^۵

روشن شد که جنگ اطلاعاتی در کدام فضا و در چه میدانهایی رخ می‌دهد. پرسش دیگر این است که چگونه چنین جنگی در حوزه نبرد نامتقارن به وقوع می‌پیوندد. به عبارت دیگر باید گفت چگونه مراحل پنجگانه یاد شده در جنگ نامتقارن به وجود می‌آید.

۱- Penetration

۲- Exploitation

۳- Destory of information

۴ - Destroy of information systems

۵ - Destruction of vital and critical infrastructures



الف) نفوذ

اولین مرحله از جنگ اطلاعاتی، نفوذ و رخنه در شبکه‌های اطلاعاتی دشمن است. این اقدام هر چند نخستین مرحله از جنگ به شمار می‌آید ولی در واقع مهمترین مرحله جنگ نیز محسوب می‌گردد. اصولاً بدون رخنه به شبکه‌های اطلاعاتی دشمن، نمی‌توان نبردی را شکل داد. در این مرحله، نفوذ باید به شکلی صورت گیرد که بدون ایجاد هیچ گونه هشدار برای دشمن باشد. در این مرحله جنگجویان جنگ اطلاعاتی می‌کوشند تا بدون ایجاد هرگونه حساسیت در سیستم‌های اطلاعاتی دشمن نفوذ کنند و در آنجا مکان مناسب را برای آشیانه کردن به شکل پنهان بیابند. این مرحله از جنگ می‌تواند بنیادی‌ترین مرحله را شکل دهد و در صورت موفقیت، نیروی مهاجم را به پشت خطوط خودش منتقل نماید.

نفوذ در شبکه‌های اطلاعاتی دشمن، فقط آن هنگام می‌تواند رخ دهد که این شبکه‌ها را بتوان از طریقی به نوعی از سیستم‌های قابل دسترس متصل نمود. این امر به دو شیوه امکان‌پذیر می‌گردد: یا دشمن به منظور بهره‌برداری و به دست آوردن اطلاعات و یا هر گونه هدف دیگر به یک شبکه دیگر متصل گردد یا این که از طریق ارائه نرم افزارهای لازم از طریقی که برای وی هشدار را ایجاد نماید در سامانه اطلاعاتی او رخنه نمود.

با وجود تمهیدات فراوانی که در این زمینه به وجود آمده است دو مقوله جنگ شبکه‌ای و جنگ نرم‌افزاری، آنچنان گسترده گردیده که نمی‌توان در هیچ وضعیتی امکان نفوذ دشمن را در سیستم‌ها نادیده انگاشت.

حتی کشورهای غربی، بویژه کشوری مانند آمریکا که خود به وجود آورنده چنین سامانه‌هایی هستند امروزه در سطحی بسیار کلان با این مشکل روبه رو می‌باشند.

اداره حسابرسی آمریکا^۱ (GAO) هر ساله آماری از حملات و رخنه‌های صورت گرفته در شبکه‌های اطلاعاتی پنتاگون و سیا را منتشر می‌کند و ضریب موفقیت و یا ناکامیهای مهاجمان را نیز ارزیابی و ارائه می‌نماید.

ب) بهره‌وری

پس از نفوذ در سیستم‌های اطلاعاتی و پس از یافتن مکانی مناسب برای استقرار امن در این نوع سامانه‌ها نوبت به بهره‌برداریهایی اطلاعاتی از اطلاعات دشمن فرامی‌رسد. روشن است که هر گونه اطلاعاتی می‌تواند در این مرحله جمع‌آوری گردد. چه بسا این اطلاعات در آینده‌ای نه چندان دور و در مسیر جمع‌آوری اطلاعات دیگر بسیار مفید و ارزشمند باشد. بهره‌برداری از اطلاعات دشمن در مرحله نخست با به دست آوردن ارتباطات اطلاعاتی در سیستم‌های اطلاعاتی دشمن بسیار حائز اهمیت بوده و می‌تواند راه را برای کسب اطلاعات دیگر سیستم‌ها نیز باز نماید. از سوی دیگر مخازن اطلاعات دشمن نیز همیشه از اهداف استراتژیک محسوب می‌گردد. در چنین مرحله‌ای است که دستیابی به این مخازن ممکن است اطلاعاتی را در اختیار قرار دهد که حتی با انجام عملیاتهای پنهان اعزام جاسوس و استخدام عامل، این اطلاعات قابل دسترسی نباشد همانطور که قبلاً گفته شد در جنگهای اطلاعاتی امروزی، پایگاههای اطلاعاتی در فضای سایبری بیشتر هدف قرار می‌گیرند و تأکید کمتری بر جمع‌آوریهای اطلاعاتی انسانی و یا اطلاعات الکترونیک صورت می‌پذیرد.

ج) تخریب اطلاعات

تخریب اطلاعاتی از جمله اهداف حمله به سیستم‌های اطلاعاتی دشمن است. از بین بردن اطلاعات دشمن در هر مرحله می‌تواند بسیاری از طرحها و برنامه‌های

۱ – Governmental Accountability (GAO)



استراتژیک دشمن را از بین برده یا به تعویق اندازد. سازمانها و گروهها و یا کشورهای کوچک در برابر کشورهای قویتر همواره از تخریب اطلاعات سود جسته‌اند. در جای خود خواهیم گفت آنچه امروزه به عنوان تخریب اطلاعات صورت می‌پذیرد چگونه می‌تواند آسیب‌های گرانی را بر یک مجموعه یا یک نظام وارد آورد. بویژه تخریب اطلاعات در مجموعه جنگ اطلاعاتی از مراحل پرهزینه برای دشمن به شمار می‌آید. تخریب اطلاعات در سیستم‌های پردازش اطلاعات و سامانه‌های ارزیابی و تحلیل اطلاعات و در بانکهای اطلاعاتی این سیستم‌ها صورت می‌گیرد. چنین عملیاتی می‌تواند همانگونه که ضربات جدی بر دشمن وارد می‌سازد، در حین عملیات سرنخ‌هایی را برای آسیب‌پذیری در اختیار دشمن قرار دهد. از آنجا که جنگ اطلاعاتی بیشتر به ضربه زدن به دشمن اطلاق می‌شود باید دانست که حفظ اطلاعات خودی نیز دارای اهمیت ویژه می‌باشد.

اما این که چگونه تخریب اطلاعات در سیستم‌ها به شکل فنی صورت می‌پذیرد از بضاعت این نگارنده خارج است. تا این اندازه می‌توان اشاره کرد که جنگ شبکه‌ای و جنگ نرم افزاری در هر سطح آن می‌تواند به تخریب اطلاعات نیز منجر شود. با وجود این، تخریب اطلاعات بیشتر به حوزه‌های ارتباطات منطقی میان اطلاعات مربوط می‌گردد. تخریب فایل‌های اطلاعاتی، جایگزین کردن فایل‌های مبهم، و مغشوش کردن این فایل‌ها و زمان ظهور آنها از این جمله‌اند.

تخریب اطلاعات دشمن در موارد فنی و علمی‌گاه با جایگزین کردن برخی اطلاعات نادرست و ایجاد فریب در ذهن کاربران شکل می‌گیرد. جایگزین کردن اعداد و ارقام دیجیتالی در سیستم‌های فنی و علمی می‌تواند مشکلات جدی و فزاینده‌ای را برای کاربران آنها به وجود آورد. اصولاً باید متذکر شد که ایجاد این تخریب فقط با از بین بردن اطلاعات و یا تخریب سیستم‌های آنها صورت نمی‌گیرد بلکه

گاهی با قراردادادن برخی از ویروسها به عنوان عمل کننده در سیستمهای پردازشی اطلاعات در حین کاربری صورت می گیرد.

(د) انهدام سامانه های اطلاعاتی

سیستم های اطلاعاتی هر یک دارای ویژگی ها، فرمت ها و برنامه های پایه ای خاص خود می باشند. اطلاعات در این سامانه ها به نحوی تعریف، طبقه بندی و با یکدیگر مرتبط می گردند. از آنجا که هر فرمتی در سیستم خود دارای مختصات ویژه ای است بدیهی است که از بین بردن این مختصات و یا مخدوش کردن آنها می تواند یک سیستم اطلاعاتی را کاملاً مورد آسیب قرار دهد. در جنگ اطلاعاتی، از بین بردن سامانه های اطلاعاتی می تواند هم سیستم و هم اطلاعات دشمن را تخریب نماید. جنگ اطلاعاتی یعنی:

«عملیاتی که برای دستیابی به برتری اطلاعاتی با تحت تاثیر قراردادن اطلاعات دشمن، فرایندهای اطلاعات پایه، سیستم های اطلاعاتی و شبکه های رایانه ای در ضمن دفاع از اطلاعات خود و فرایندهای اطلاعات پایه ای خود و سیستم های اطلاعاتی و شبکه های اطلاعاتی خودی تعریف می گردد.»

همانگونه که در این تعریف ذکر گردیده است با توجه به فرایندهای اطلاعات پایه ای در سیستم های اطلاعاتی و شبکه های رایانه ای می توان ضمن دفاع از اطلاعات خود، سامانه های اطلاعاتی دشمن را نیز مورد تهاجم قرار داد تا امکان دستیابی به برتری اطلاعاتی فراهم گردد. این سامانه ها در شبکه های رایانه ای دشمن و خودی نقش اردوگاهها و پایگاههایی را ایفا می کنند که اطلاعات و جنگجویان اطلاعاتی در آن استقرار یافته اند.

برای از بین بردن سیستم های اطلاعاتی، نخست باید از مرحله نفوذ عبور کرد. بسیاری بر این عقیده هستند که امروزه می توان حتی بدون نفوذ و صرفاً با ایجاد یک



درگیری شبکه‌ای به انهدام سامانه‌های اطلاعاتی دست یازید. با پیشرفتهای فناوری می‌توان گفت که این امر امروزه قابل تحقق است و بخصوص هنگامی که با نفوذ در سامانه اطلاعاتی دشمن و شناخت اطلاعات و شناسایی پایگاههای اطلاعاتی دشمن همراه باشد.

هـ) انهدام زیرساختهای حیاتی و حساس

یکی دیگر از صحنه‌های جنگ اطلاعاتی، تأسیسات و زیرساختهایی هستند که با سیستم‌های اطلاعاتی، مدیریت و کنترل می‌شوند. امروزه کلیه زیرساختهای حیاتی و حساس کشور از قبیل تأسیسات انرژی، حمل و نقل، سلامتی و بهداشت، ذخیره آبرسانی و ... با سامانه‌های کنترلی اطلاعات، هدایت می‌گردند.

در هر جنگی برای طرفهای درگیر، از بین بردن و یا فلج ساختن این گونه تأسیسات می‌تواند بسیار کلیدی باشد. بمبارانهای صورت گرفته در طول جنگها با هدف تخریب نیروگاهها، سدها، پلها، سیستمهای مخابراتی و ارتباطی همه و همه اهمیت فراوان این تأسیسات را در پشتیبانی افزایش توان استراتژیک یک کشور نشان می‌دهد. با توجه به پیشرفتهای شگفت آور در عرصه‌های مدیریت اطلاعاتی، تقریباً کلیه سیستم‌های ذکر شده با اداره یک مرکز اطلاعاتی هدایت و کنترل می‌گردند.

به هر صورت جنگجویان جنگ اطلاعاتی به خوبی دریافته‌اند که از این طریق می‌توانند ضربات و صدماتی را وارد نمایند که حتی در بمبارانهای استراتژیک نیز به آسانی قابل دستیابی نبوده‌اند. در دهه اخیر نمونه‌های فراوانی از این نوع جنگ دیده شده است. با ورود به این سامانه‌های اطلاعاتی و تخریب اطلاعات کنترلی آنها و از بین بردن فرایندهای اطلاعاتی پایه‌ای، وضعیت کنترل سیستم‌های انرژی، حمل و نقل، مخابرات و ارتباطات کاملاً مغشوش و آسیب‌های چند میلیارد دلاری بر این سیستم‌ها وارد می‌شود. قطع برق، به هم خوردن برنامه حرکت و هدایت قطارها، از بین رفتن سیستم‌های هدایت و کنترل امواج مخابراتی و ارتباطاتی، مغشوش کردن

سیستم‌های توزیع آبرسانی، متوقف ساختن حرکت پلهای متحرک و... همه و همه به تخریب و انهدام تأسیسات و زیرساختهایی می‌انجامد که جبران هر یک از آنها، ماهها و گاهی سالها به طول می‌انجامد. به هر حال جنگ با هدف از بین بردن تأسیسات حیاتی و حساس ملی یک کشور همیشه از نگرانیهای اصلی فرماندهان جنگی بوده است. تاریخ جنگ‌ها از بمبارانها و حملات توپخانه‌ای، تخریبهای چریکی و... برای از بین بردن این گونه تأسیسات، سخن‌های فراوان دارد؛ اما در جنگ اطلاعاتی این تأسیسات با حملات و تهاجم آرامی، آسیب‌های گرانی می‌بینند.

به هر حال هنگامی که تأسیسات حیاتی و حساس در کشورها در یک نظام کنترلی اطلاعاتی هدایت می‌شوند، آسیب‌پذیری این سیستم‌ها تابعی از آسیب‌پذیری سامانه‌های اطلاعاتی می‌گردد و این امر یکی از میدان‌های جنگ اطلاعاتی را گسترش می‌دهد که آن میدان، معرکه جنگ اطلاعاتی در زیرساختها و تأسیسات حیاتی و حساس است.

جنگ نامتقارن

بسیاری بر این باورند که جنگ نامتقارن از پدیده‌هایی است که توانسته قدرتهای بزرگ را متوجه ضعف‌ها و سیستمهای خود نماید و قدرتهای کوچک‌تر را برای بهره‌برداری از این نقاط ضعف و آسیب‌ها با انگیزه‌تر سازد. سخن گفتن از تهدیدات نامتقارن مقدم بر جنگ نامتقارن است ولی تا اندازه‌ای این دو مفهوم با یکدیگر نزدیکی و قرابت پیدا کرده‌اند که نمی‌توان به طرح یکی بدون دیگری پرداخت. جنگ نامتقارن در واقع حالت بالفعل تهدیدات نامتقارن است. تهدید نامتقارن از سوی یک گروه یا سازمان یا کشور ضعیفتر متوجه کشور قدرتمندتر می‌گردد؛ در حالی که جنگ نامتقارن می‌تواند از هر دو سو آغاز گردد و یا شکل گیرد.



در این میان برخی تقسیم بندیهای دیگر نیز در حوزه تهدیدات نامتقارن به چشم می‌خورد. برخی، تهدیدات را با توجه به ارزش هدف مورد تهدید، سطح بندی و تعریف می‌کنند. یکی از کارشناسان برجسته در این زمینه می‌نویسد :

« برخی بر این باورند که تهدیدات بایستی بر اساس اهمیت هدف مقوله‌بندی گردد. در مورد تهدیدات پدیدار شده در یازدهم سپتامبر می‌توان آنها را به روشنی در سطح استراتژیک طبقه‌بندی کرد درحالی که تهدیدات از نوع حمله به ناویو. اس. اس. کول در یمن را باید در سطحی تاکتیکی طبقه بندی نمود.» (بالک، ۲۰۰۳، ص ۶)

با وجودی که می‌توان این تعریف را پذیرفت اما نمی‌توان هر تهدید نامتقارنی را تهدید استراتژیک تلقی کرد. در این صورت تحقق آن تهدید هم نمی‌تواند یک جنگ استراتژیک را شکل دهد. با توجه به این نکته جای این پرسش باقی است که تهدیدات مورد نظر در جنگ اطلاعاتی چه نسبتی با سطوح استراتژیکی و تاکتیکی در جنگ نامتقارن پیدا می‌کنند؟ به عبارت دیگر اصولاً تهدیدات مورد نظر در یک نوع جنگ اطلاعاتی در چه صورت می‌تواند به تهدیدی جدی در جنگ نامتقارن تبدیل گردد. اصولاً این نوع تهدید و این نوع جنگ چه نسبتی با جنگ متقارن پیدا خواهد کرد.

جنگ نامتقارن بنا به تعریف، در صورتی می‌تواند نوعی جنگ باشد که در آن اساساً عمل، سازماندهی و تفکر کاملاً متفاوت از روش دشمن برای به حداکثر رساندن امتیازات خود و بهره‌برداری از نقاط ضعف دشمن، دستیابی به ابتکار یا یافتن آزادی عمل بیشتر صورت گیرد. (متز و جوهسون، ۲۰۰۱، صص ۳-۱۲) در این حالت می‌توان امتیازات خود را در سطوح استراتژیک نیز در یک جنگ اطلاعاتی، درون جنگ نامتقارن به حداکثر رسانید و از نقاط ضعف دشمن بیشترین بهره‌برداری را نمود.

با اندک تأملی می‌توان دریافت که تهدیدات نامتقارن - به معنای نوعی تهدید که از تقویت امتیازات خودی برخوردار می‌گردد و از کاستی‌ها و ضعفهای دشمن

بهره‌برداری می‌نماید- در صورت تحقق می‌تواند نوعی جنگ نامتقارن را در سطح تاکتیکی، با توجه به اهمیت و سطح ضربه‌پذیری دشمن تعریف کند. جنگ اطلاعاتی که در حوزه‌های متفاوت و گوناگون و در سطوح مختلف تحقق می‌پذیرد می‌تواند به صورت غافلگیر کننده اهدافی را مورد تهاجم قرار دهد و صحنه‌ها و میدان‌های متنوعی را به وجود آورد.

از حمله به یک سیستم الکترونیک با هدایت سامانه‌های اطلاعاتی در یک ناو تا ورود به پیچیده‌ترین شبکه‌های رایانه‌ای وزارتخانه‌های دفاع و اطلاعات و ضربه زدن به اطلاعات و سیستم‌های اطلاعات پایه آنها، می‌توان این جنگ را گسترش داد. جنگ اطلاعاتی می‌تواند بسیار زودتر و سریعتر از جنگ مدرن و کلاسیک آغاز گردد و حتی به صورتی بسیار وسیعتر از ضربات فیزیکی در جنگ نامتقارن عمل کنند. با این توجه، جنگ اطلاعاتی می‌تواند به اشکال ذیل رخ دهد :

۱- جنگ اطلاعاتی پیش از جنگ نامتقارن

کشورها و گروه‌های درگیر در جنگ اطلاعاتی بسیار زودتر از وقوع جنگ کلاسیک و یا حتی نبرد نامتقارن، به جنگ یکدیگر رفته‌اند. آنها در این نوع جنگ با نفوذ در شبکه‌های یکدیگر، دستیابی به اطلاعات، بهره‌برداری از این اطلاعات و تخریب سامانه‌های اطلاعاتی و ضربه زدن به سیستم‌های هدایتی اطلاعات پایه تأسیسات حیاتی و حساس عملاً جنگ را شکل داده و تهدیدات نامتقارن را در جنگ اطلاعاتی به حالت بالفعل درآورده‌اند.

گزارش‌های متعددی از وزارت دفاع آمریکا به دست رسیده که نشانگر آغاز جنگ اطلاعاتی در یکی از مراحل بالا به این کشور بوده است. براساس گزارش وزارت دفاع آمریکا در سال ۱۹۹۹ تقریباً بین هشتاد تا صد حمله به طور روزانه یا ۲۰۰۰۰ حمله در طول سال به سیستم‌های رایانه‌ای صورت گرفته است. این گزارش



نشان می‌دهد که در هفت ماه اول سال ۲۰۰۰ تعداد ۱۴۰۰۰ حمله سایبری به سامانه‌های اطلاعاتی پنتاگون صورت پذیرفته است. (گارامون، ۲۰۰۱) شمار روزافزون این حملات و تعداد درگیری‌های فزاینده میان سایتهای متعلق به کشورها با گروه‌ها و بالعکس، نشانگر سطحی از جنگ اطلاعاتی است که هم اکنون در جریان است. این جنگ با وجود آن که بسیار خاموش است ولی آسیب‌ها و تلفات خود را وارد کرده است و دشمن را در میدانهای مختلف مورد صدمه قرار می‌دهد.

جنگ اطلاعاتی پیش از جنگ نامتقارن در سطح نفوذ و بهره‌برداری از اطلاعات می‌تواند همواره با عنوان یک حرکت پیش‌دستانه و ابتکاری، برای ورود به جنگ نامتقارن به شمار آید. داشتن اطلاعات دقیق از دشمن و دانستن و شناختن سامانه‌های اطلاعاتی او می‌تواند در هر زمانی که تصمیم گیرندگان صلاح بدانند با وارد کردن ضربات اساسی به عنوان پیش درآمد یا تکمیل کننده حملات نامتقارن به کارگرفته شود.

۲- جنگ اطلاعاتی در جنگ نامتقارن

اگر بتوانیم جنگ نامتقارن را در شیوه‌ها و روشهای گوناگون آن باز تعریف کنیم درمی‌یابیم که در این نوع جنگ دست کم در سه سطح نیرویی، فناورانه و لجستیکی میان طرفین درگیر، نوعی عدم همترازی دیده می‌شود. دو طرف درگیر دارای شمار نیروی یکسان نبوده و این نیروها حتی از نظر سطح آموزش‌ها و تکنیک‌های فردی با یکدیگر همسان نیستند. ناهمترازی میان طرفین به لحاظ فناوری نیز از مهمترین موارد عدم تقارن‌ها میان طرفهای درگیر است. به کارگیری نیروی انسانی و تجهیز امکانات و آماده‌سازی‌های فیزیکی توان رزمی که در یک عبارت لجستیک را شکل می‌دهد نیز میان طرفین به طور یکسان و همتراز وجود ندارد. جنگ اطلاعاتی در هر سه سطح ناهمتراز میان طرفین می‌تواند دخالت مؤثر و کارآمد داشته باشد و جنگ نامتقارن را شکل دهد. در این نوع جنگ به دلیل وجود فضای

سایبری، بسیاری از ویژگیهای عرصه‌های واقعی و فیزیکی می‌تواند با ویژگیهای مجازی و سایبری جایگزین گردد. البته بسیاری بر این باورند که اصولاً عملیات اطلاعاتی در محیط نامتقارن دارای مشکلات و پیچیدگی‌های خاص خود است ولی شکست‌ناپذیر نیست. گفته شده است که :

« عملیات اطلاعاتی در محیط نامتقارن مشکل ساز است ... اما غیر قابل عبور و چیرگی ناپذیر نیست. » (رانفلت و آرگویلا ، ۲۰۰۱، ص ۲)

این گفته «رانفلت» نشانگر آن است که عملیات اطلاعاتی در چنین محیطی کاملاً ویژگی‌های خاصی را داراست و نمی‌توان این محیط را با محیط‌های کلاسیک و حتی مدرن مقایسه کرد. با این وصف باید توضیح داد که در سطوح نیرویی، فناوری و لجستیکی چگونه جنگ اطلاعاتی و بهره‌برداری از فضای سایبری می‌تواند چهره جنگ را عوض نماید. یکی از نویسندگان و کارشناسان برجسته در این زمینه می‌نویسد : «گسترش شبکه‌ها و انجام عملیات اطلاعاتی در یک محیط نامتقارن به روشنی در برگیرنده خطرات و خطرپذیریهای نوینی است. روشهای نوین برای مراقبت، مونیتورینگ و حمل و نقل گسترش می‌یابند. تأسیسات حیاتی ملی انرژی، ارتباطات، حمل و نقل و همچنین سامانه‌های اطلاعاتی و سیستم‌های اطلاعات پایه حساس اقتصادی برای پشتوانه سیستم‌های مالی و بهداشتی در برابر تروریستهای سایبری و هک‌های رایانه‌ای آسیب‌پذیر باقی می‌مانند.» (پاترسون، ۲۰۰۲)

همانگونه که اشاره شده است در این صحنه، جنگجویان اطلاعاتی با انجام عملیات در زمینه‌های متفاوت اطلاعاتی و تهاجم به زیرساختها و تأسیسات حیاتی ملی می‌توانند خطرات بسیار جدی را برای دشمن خود به وجود آورند. اما باید بدین نکته آگاه بود که جنگیدن در چنین فضایی، سربازان و نیروهای متخصصی را نیاز دارد که به زعم آمریکاییان، آنها تروریستهای سایبری و یا هک‌های رایانه‌ای می‌باشند.



به روشنی پیداست که نیرو و وضعیت عدم تقارن نیرویی در این نوع جنگ، کاملاً با جنگهای کلاسیک و مدرن متفاوت است.

نیروها و افرادی که در جنگ کلاسیک با استراتژیهای عملیاتی متفاوت، بسیار سرنوشت ساز محسوب می شدند و در صورت تصرف فیزیکی یک منطقه می توانستند در تحمیل اراده بر دشمن بسیار مؤثر باشند و یا با انجام عملیاتهای تخریبی درون شهری دشمن و یا پشت خط جبهه ها بسیار کارآمد عمل نمایند، یکی از مهمترین عوامل ناهمترازی را میان دو طرف درگیر به وجود می آورند. جنگ اطلاعاتی در جنگ نامتقارن فقط با بهره برداری از جنگجویان سایبری و هکرها متخصص و از طریق جنگ شبکه ای ضربات و صدمات خود را بر همان سامانه ها و سیستم ها و زیرساختهای حیاتی ملی دشمن وارد آورده و گاه با ورود به سیستم های رایانه و کنترلی، موجبات اغتشاش و انهدام سیستم های C4I را نیز در فرماندهی های صحنه های عملیاتی به وجود می آورند.

بهره برداری از دو عنصر فضای مجازی^۱ و گمنامی شبکه ای^۲، محیطی را به وجود می آورد که هکرها و جنگجویان اطلاعاتی بتوانند به طور بسیار کارآمدی، ناهمترازی میان دو ارتش را از لحاظ نیرویی و پرسنلی جبران نمایند. این دو پارامتر هر کدام به نوبه خود یکی از مهمترین عوامل را برای درگیرکردن یک سیستم شبکه ای با یک انبوه سازمانی به وجود می آورد. این امر باعث می شود طرفین درگیر در ردیابی های اطلاعاتی با مشکلاتی جدی رو به رو گردند که ذکر مفصل آن از حوصله این مقاله بیرون است.

۱- Virtual space

۲- Network Anonymous

سطح دوم از جنگ اطلاعاتی در جنگ نامتقارن، جنگ اطلاعاتی در حوزه فناوری است. در گذشته‌ای نه چندان دور هنگامی که سخن از جنگ در صحنه‌های نبرد به میان می‌آمد از نوعی نبرد به نام جنگ الکترونیک سخن گفته می‌شد. این نوع جنگ که هنوز هم بسیار متداول و قابل اجراست طیفی از عملیاتهای یک طرف علیه طرف دیگر را در حوزه‌های الکترونیک فرامی‌گرفت. امروزه برخی برآنند که جنگ الکترونیک در جنگ اطلاعاتی نهفته است و یا آن که اصولاً جنگ اطلاعاتی چیزی بیش از همان جنگ الکترونیک نیست. هر چند با اندک تأملی می‌توان دریافت که چنین چیزی صحیح به نظر نمی‌رسد ولی می‌توان این سخن را در این حد پذیرفت که جنگ الکترونیک یکی از پایه‌های اصلی جنگ اطلاعاتی را تشکیل داده است.

جنگ اطلاعاتی را در حوزه فناوری می‌توان دست مایه‌ای برای پرکردن شکافهای فناوری میان دو طرف درگیر و فاصله آن میان آنها دانست. روشن است که بهره‌مندی از فناوری بسیار پیچیده‌تر، می‌تواند یک طرف را در درگیری‌های میدان نبرد کامیاب‌تر سازد. اما این، همه داستان نیست. به هر حال به کارگیری فناوری نیز به عنوان یک برتری یا امتیاز می‌تواند خود تابعی از شرایط و عوامل و عناصر بسیاری باشد که جنگ اطلاعاتی به راحتی این شرایط و عوامل و عناصر را مورد هدف قرار می‌دهد. بدیهی است که با هدف قراردادن عواملی که به کارگیری فناوری به آنها بستگی تامی دارد می‌تواند ضریب بالایی از برتری فناوری را کاهش دهد. امروزه این امر به سادگی امکان‌پذیر گردیده است.

ورود به شبکه‌های کنترل سیستم‌های هدایتی فناوریهای پیشرفته، به کارگیری وسایل و ابزار غیرنظامی برای حمله به اهداف نظامی، گزینش مراکز علمی و فنی برای هدف قرار دادن، استفاده از توانمندیهای فنی در ضربه زدن به سیستمهای پشتیبانی کننده نظامی و غیرنظامی، ایجاد اختلال در شبکه‌های رایانه‌ای هدایت



سیستم‌های موشکی، کشتیرانی، تلویزیونی، تعیین موقعیت و ... همه و همه از جنگ افزارهایی هستند که جنگجویان اطلاعاتی، آنها را در جنگ اطلاعاتی در نبردهای نامتقارن برای بهره‌مندی از برتریهای خودی با بهره‌برداری از ضعفها و کاستی‌های دشمن به کار می‌گیرند.

جنگ اطلاعاتی در حوزه فناوری هرچند مختصات و ویژگی‌های فنی بسیاری دارد ولی از آن حیث که از طریق سیستم‌های رایانه‌ای در فضای سایبری تحقق می‌پذیرد جنگی نامتراز و غیرقابل پیش‌بینی است. این حوزه از جنگ می‌تواند هر لحظه با خطر تهاجم رایانه‌ای هکرهای حرفه‌ای روبه‌رو گردد. پس می‌توان گفت که جنگ اطلاعاتی در جنگ نامتقارن تا اندازه‌ای نقصانها و شکافهای فناوری را نیز جبران می‌نماید.

جنگ اطلاعاتی در حوزه لجستیک نیز از مهمترین بخش‌های جنگ اطلاعاتی در جنگ نامتقارن است. در جنگهای کلاسیک و حتی مدرن نیز بمباران استراتژیک و یا اشغال زمین پس از جنگ از هوا و یا استراتژی عملیاتی جنگ بدون درگیری صورت می‌پذیرد و لجستیک نیرو و آماده‌سازی توان رزمی از مهمترین بخشهای این عملیات محسوب می‌گردد.

امروزه واحدهای درگیر در جنگ نامتقارن تلاش دارند که به نحوی از به هم پیوستگی ارتشهای کلاسیک به عنوان یک نقطه ضعف سود جسته و آنچه را که در گذشته همواره یک برتری محسوب می‌شد به عنوان یک آسیب‌پذیری به کارگیرند. نقل و انتقال در صحنه‌های نبرد و همچنین در شهرهای پشتیبان‌کننده از یک سو و حمل و نقل به عنوان یکی از فرایندهای زندگی شهری که کاملاً از سیستم‌های اطلاعاتی هدایت شونده برخوردار است، نقاط آسیب‌پذیر مناسبی را در اختیار جنگجویان اطلاعاتی قرار می‌دهد که با بهره‌برداری از آنها در جنگ نامتقارن مشکلات عدیده‌ای

را برای دشمن در صحنه‌های مختلف فراهم می‌آورد. از بین بردن برنامه‌های کنترل هواپیما، قطار، کشتیرانی، جابه جایی مسافر، کنترل ورود و خروج سیستم‌های پشتیبانی کننده نظامی و غیرنظامی از طریق یک جنگ شبکه‌ای و نرم‌افزاری، قطع برق سیستم‌های قطارهای برقی، از بین بردن کنترل‌های راداری و ... خود به خود مشکلات بسیار جدی را در لجستیک‌های نظامی و غیرنظامی به بار خواهد آورد که رفع این مشکلات در زمان خود به راحتی امکان‌پذیر نخواهد بود. خسارتهای وارده از سوی این نوع جنگها می‌تواند گاهی تا میلیاردها دلار بالغ گردد که شاید هرگز این وضعیت در سیستم‌های جنگ‌های کلاسیک با سلاح های متعارف قابل دستیابی نبوده است.

جمع‌بندی و نتیجه‌گیری :

آنچه ذکرگردید اجمالی از مباحث طرح‌شده در زمینه جنگ اطلاعاتی در جنگ نامتقارن بود. تغییر و تحولات سریع در چهره‌های جنگ‌ها، به کارگیری ابتکارات و ابداعات نوین، پیشرفتهای فناوری عصر صنعتی و عصراطلاعات، شرایط انقلاب در امور نظامی و تغییر در سمت و سوی جنگها از میدانهای نبرد فیزیکی به میدانهای نبرد اطلاعاتی موجب گردید که فرایند جنگها از سیستم‌های کلاسیک به نبردهای نوین و از آنجا به نوع جنگ موسوم به جنگ نامتقارن تغییرکند. این امر باعث شد که حرکتی شتابان دربه کارگیری فناوری اطلاعات در جنگ‌های نامتقارن به وجود آید که تا اندازه زیادی شکافهای ناشی از اختلاف سطح نیرویی و فناوری و لجستیک را پر نماید. به عبارت دیگر به راحتی می‌توان گفت که درچه شرایطی چه نوع جنگی رخ می‌دهد و چه طرفی بیش از دیگری آسیب می‌بیند. این موضوع تابعی از جنگ در حوزه‌های جنگ اطلاعاتی در جنگ نامتقارن است.



منابع فارسی :

- ۱ - بوزان، آدا، (۱۳۸۲)، «اطلاعات استراتژیک و کشورداری»، ترجمه پژوهشکده مطالعات راهبردی.
- ۲ - کاستلز، مانوئل، (۱۳۸۲)، «عصر اطلاعات ، ظهور جامعه شبکه‌ای»، ترجمه احمدعلی قلیان و افشین خاکباز، طرح نو.
- ۳ - کلهر، رضا، (۱۳۷۹)، «جنگ اطلاعاتی در جنگ آینده»، مجله سیاست دفاعی، شماره ۳۲-۳۳.
- ۴ - کلهر، رضا، (۱۳۸۰) «جنگ متقارن در دریا» ماهنامه خلیج فارس و امنیت، انتشارات نیروی دریایی سپاه، ش ۱۹.
- ۵ - مکنزی، کنت، (۱۳۸۲) «جنگ نامتقارن»، ترجمه عبدالمجید حیدری، محمد تمنایی، دوره عالی جنگ سپاه، چاپ اول ، بهار.
- ۶ - وبستر، فرانک، (۱۳۸۲) «نظریه‌های جامعه اطلاعاتی»، ترجمه مهدی داوودی، تهران، مرکز چاپ انتشارات وزارت امور خارجه .
- ۷ - هیل، مایکل (۱۳۸۱)، «تاثیر اطلاعات بر جامعه»، ترجمه محسن نوکاریزی، انتشار چاپار، تهران.
- ۸ - هیلزگری، کریس، (۱۳۷۹) «جنگ پست مدرن » ، مجله سیاست دفاعی، شماره ۳۲-۳۳.

منابع لاتین :

1. Blank, Stephen. J(2003)., “ Rethinking Asy Threats” RAND santa monica, September.
2. Garamone, Jim (2001) “joint staff Roloses information operations” Doctorire, “ Doctorire, Defrance Link American forces press”.
3. Gray, Colins (2002), Thinking Asymmetrically in times of terror” parameter, Spring.
4. Metz. Steven and Johnson, Douglas V(2001).” Asymmetry and U.S Military Strategy: Definition, Background, Strategic Concepts Carlisle Barracks, Pa. Strategic Studies institute u.s. Army war college.
5. Patterson, Lic Lawarren V(2002)., ”Information operations and asymmetric warfare Are we realy? “ Carlisle Barracks , us Army College.
6. Ronfeldt, David and Arguilla , John(2001). “ Network , Netwars and the fight for the future” 10 October.